MESA INTERNATIONAL
MANUFACTURING ENTERPRISE SOLUTIONS ASSOCIATION
MESA.ORG

Additional partner logos

Applying ISA/IEC 62443 to Control Systems

Graham Speake

Principal Systems Architect Yokogawa

MESA*KNOWS*

SUSTAINABILITY & ECO-EFFICIENCY - LEAN - METRICS & PERFORMANCE MANAGEMENT
INFORMATION INTEGRATION - SAFETY - ASSET PERFORMANCE MANAGEMENT - B2MML
QUALITY & COMPLIANCE - PRODUCT LIFECYCLE MANAGEMENT - AUTOMATION

Do you know MESA?

Graham Speake

- BSc Electrical and Electronics Engineer
- 16 years experience in computer security
- 12 Years experience in automation security
- Worked for Ford Motor Company, ICS, ATOS-Origin and BP
- Worked as an independent consultant on financial security
- Member of ISA, ISCI, ISC^2
- Principal Systems Architect at Yokogawa

YOKOGAWA

ACRONYMS

Acronyms

- SCADA, DCS, PCN, industrial automation
- PLC, embedded controller
- Process control
- HMI
- PI, Historian

Acronyms -2

- Whitelisting
- IDS
- IPS
- phising

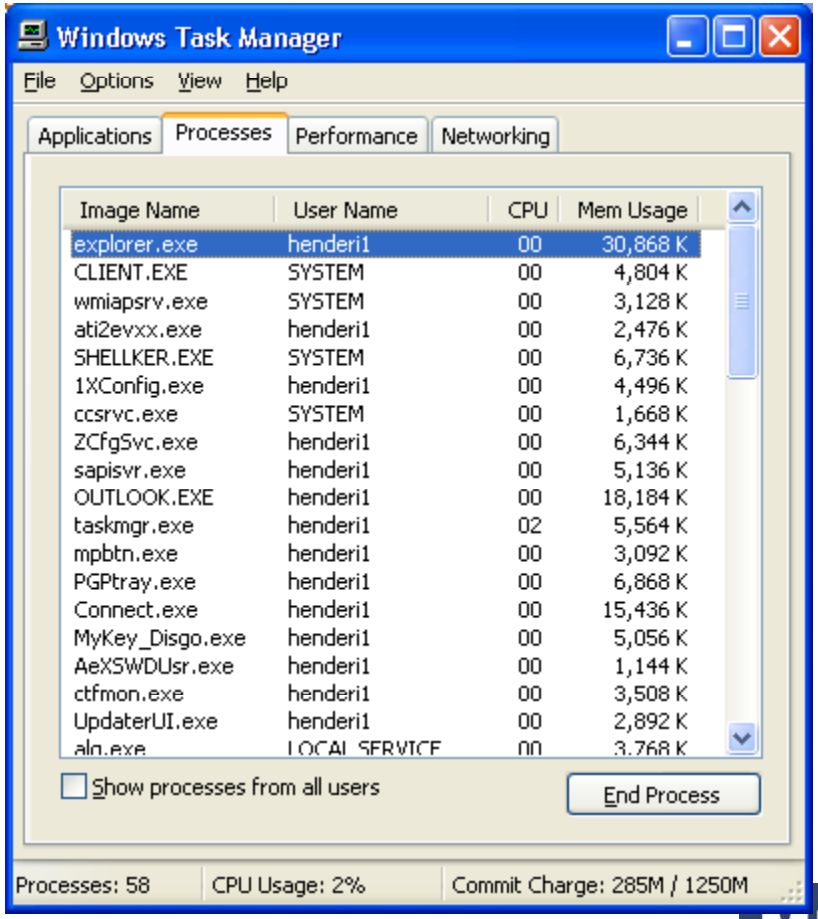
Language difficulties

I am not in the office at the moment. Send any work to be translated

PROCESS CONTROL

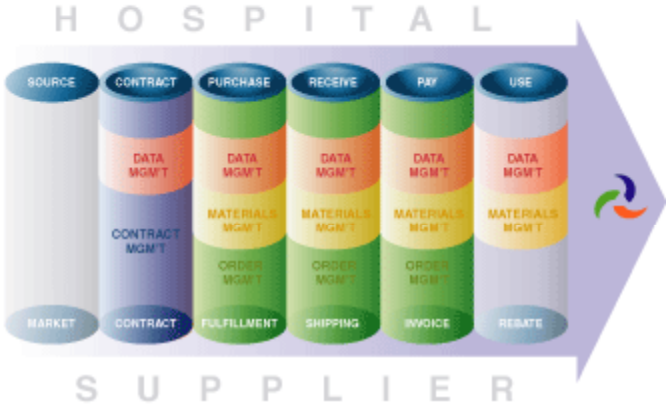
What do we mean by Process Control?

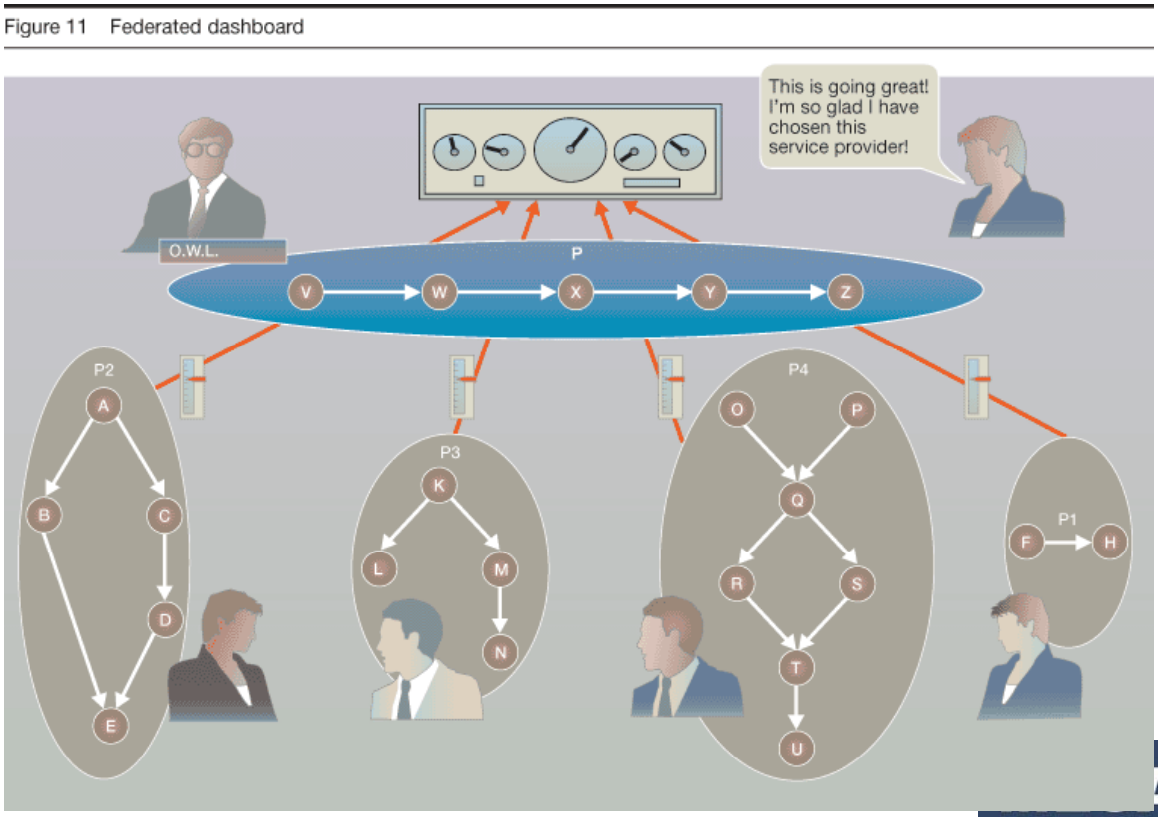
Is this process control?



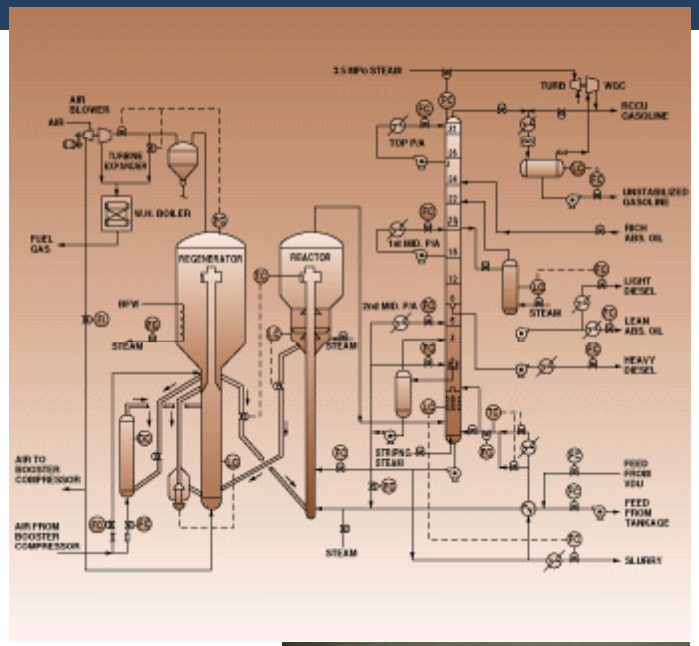
What do we mean by Process Control?

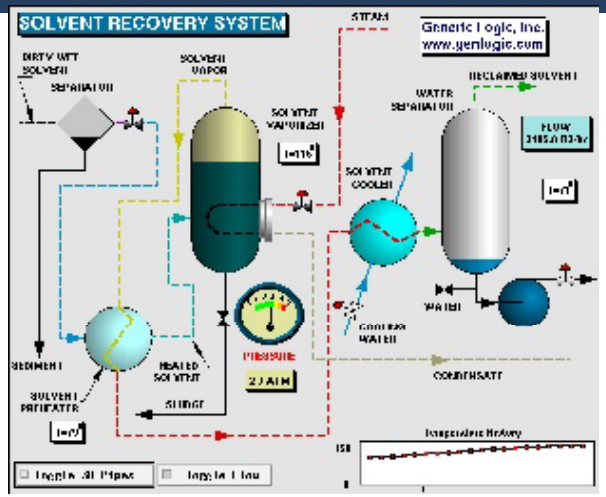
How about these?

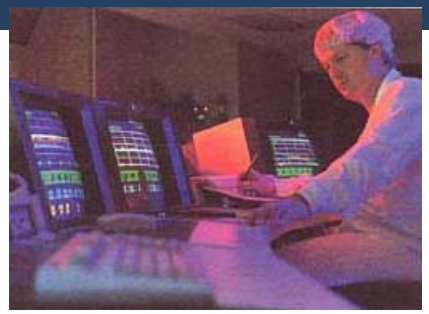




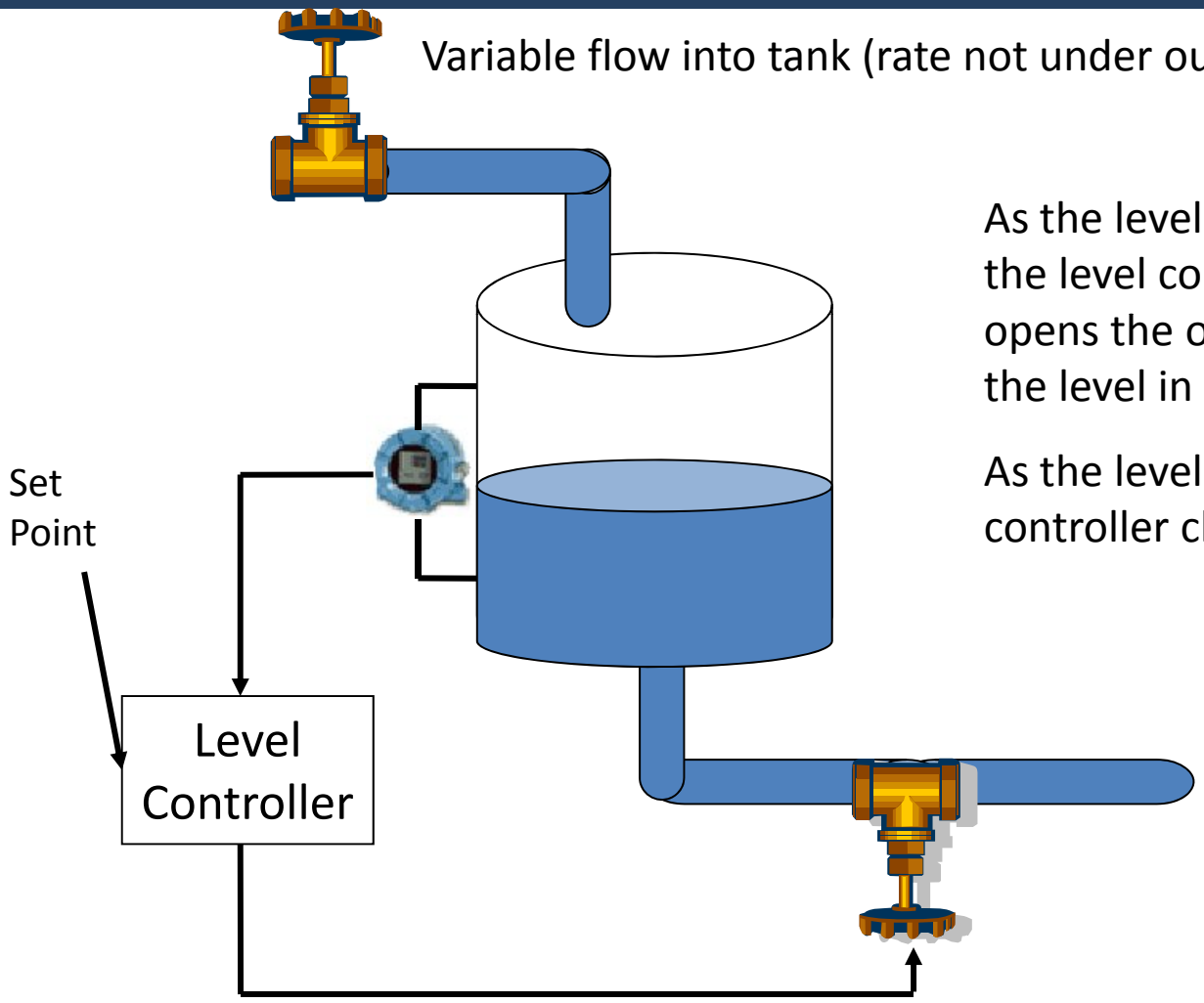
Process Control in this context is:







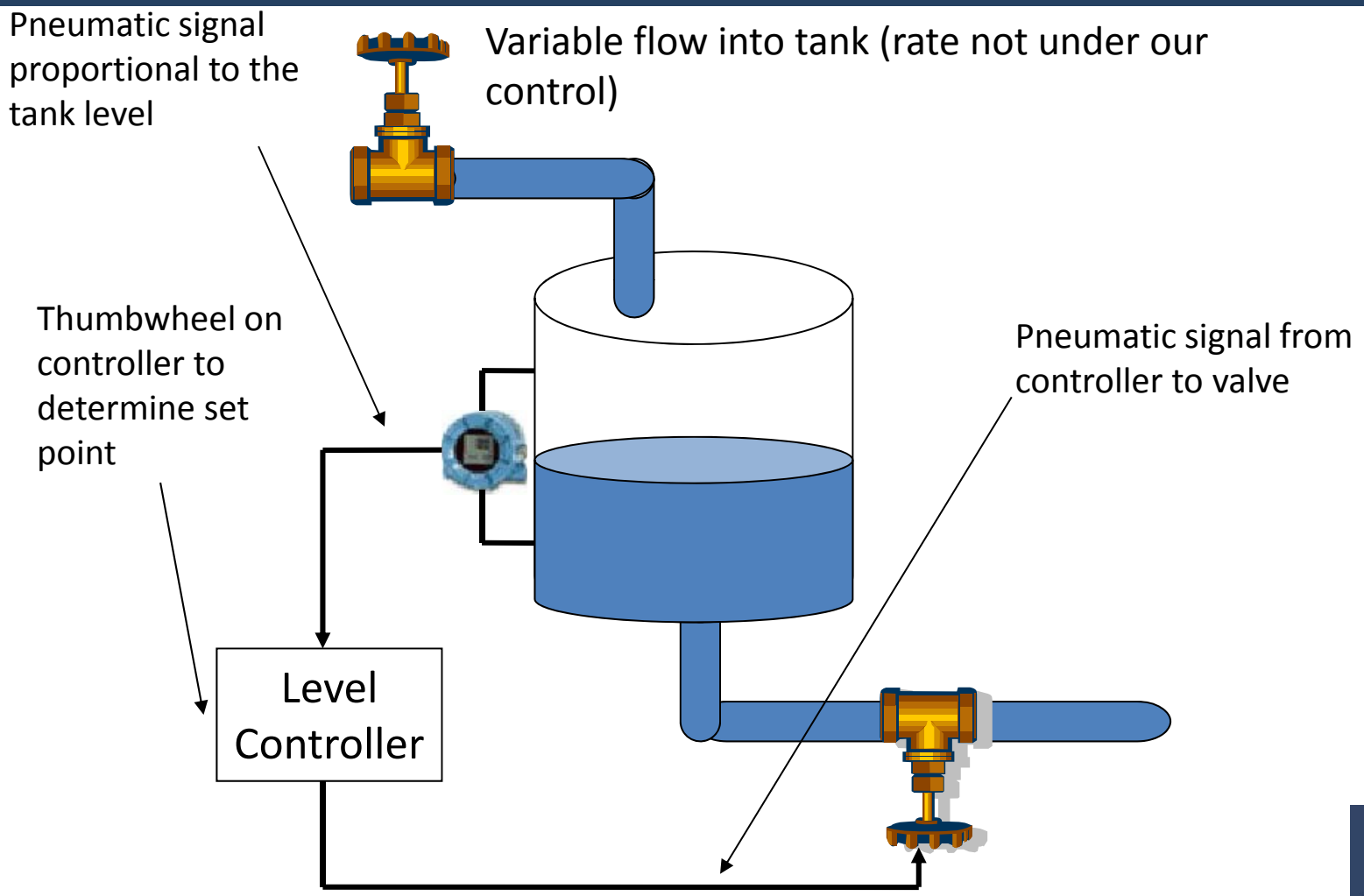
Level Control Example



As the level in the tank increases, the level controller progressively opens the outlet valve to maintain the level in the tank.

As the level decreases, the controller closes the valve

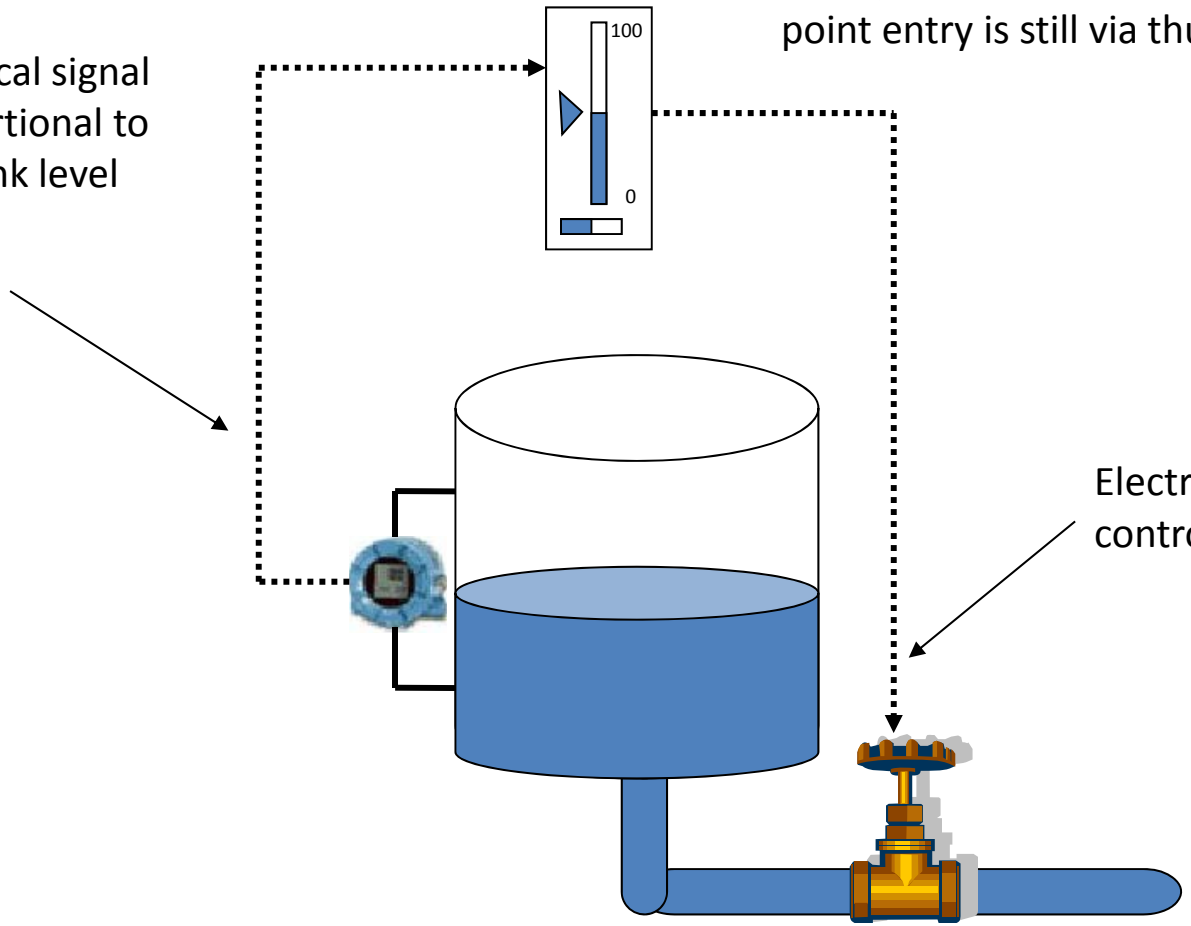
Control up to 60's



Control in the late 60's & early 70's

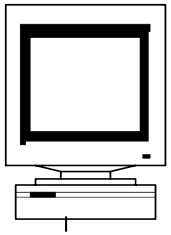
Electronic controller located remote from plant in control room. Operator set point entry is still via thumbwheel

Electrical signal proportional to the tank level



Electrical signal from controller to valve

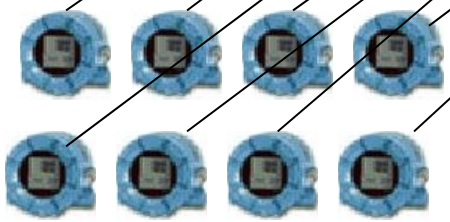
The 1970's The Distributed Control System

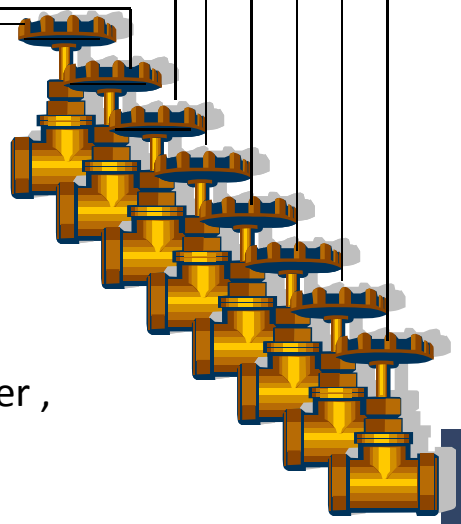


An Operator Station, level indicated on a screen, operator changes set point via keyboard for the first time!

Data Hiway

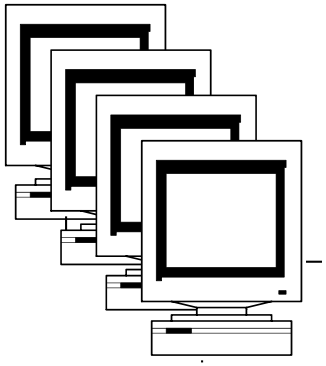
Basic Controller





Electrical signals to/from controller , controller handles 8 loop at once

The 1970's The Distributed Control System



Multiple Operator Stations, one operator can control a refining unit

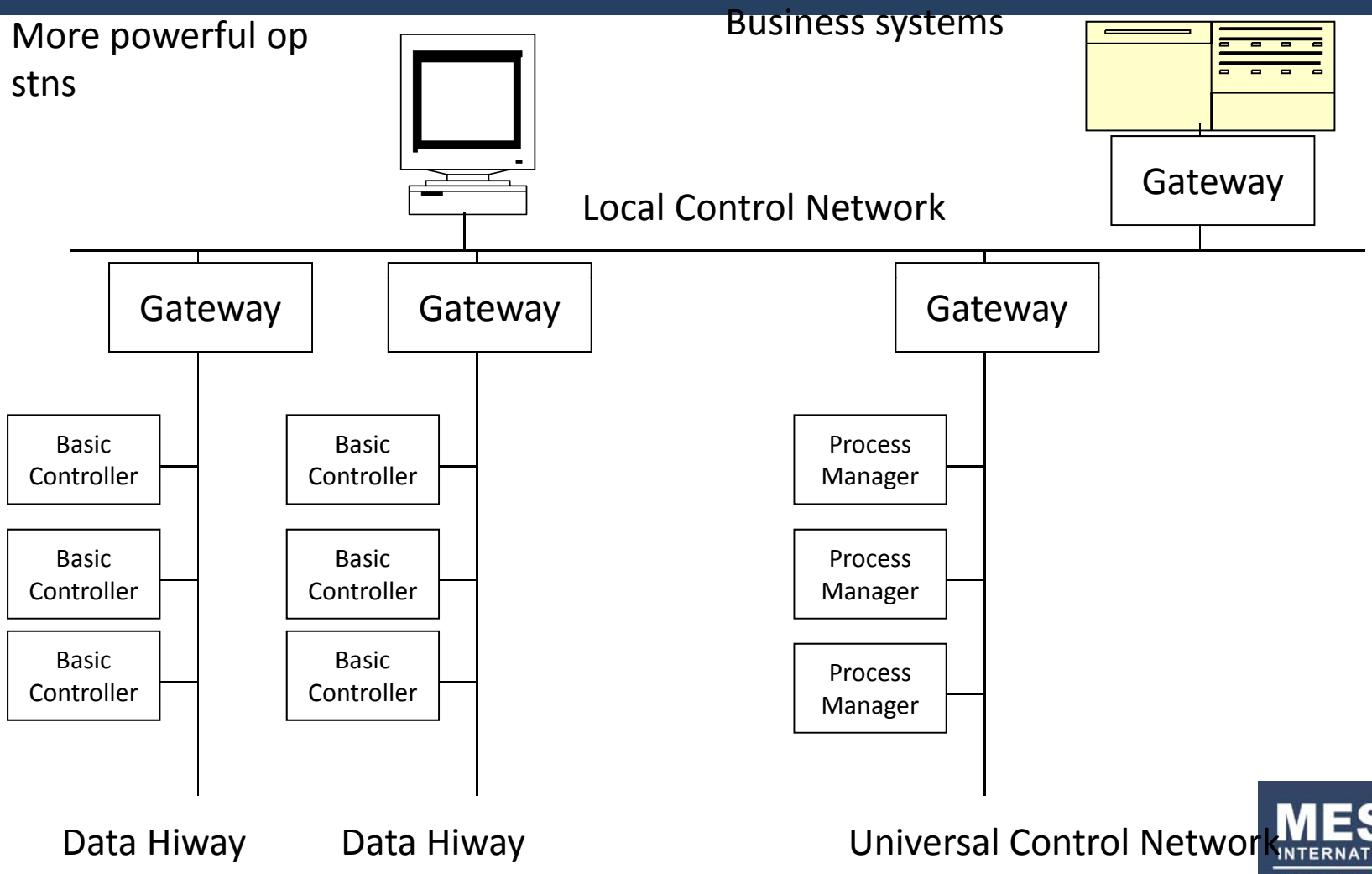
Data Hiway

Basic Controller #1

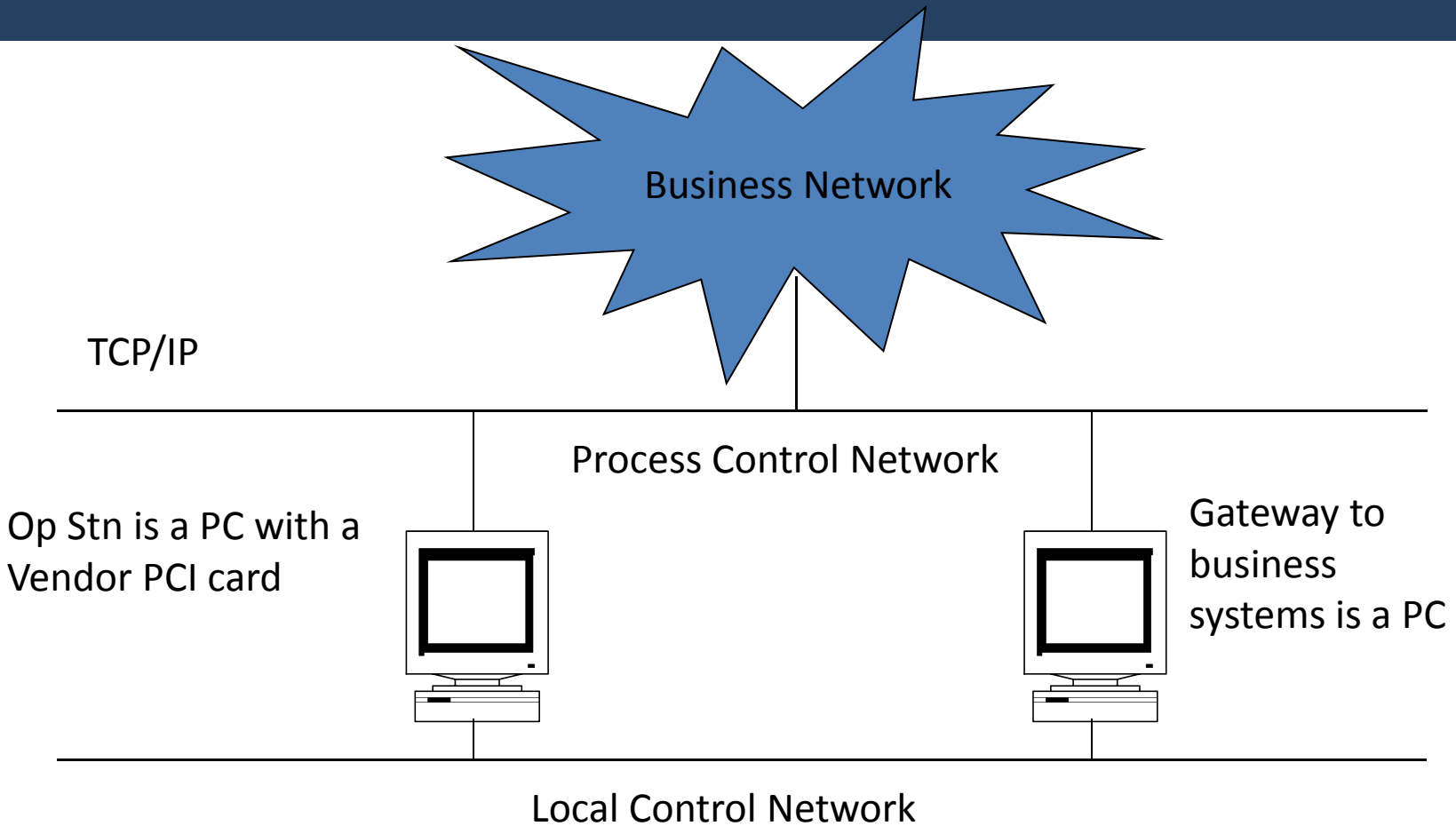
Basic Controller #2

Basic Controller #32

1980's The DCS evolves

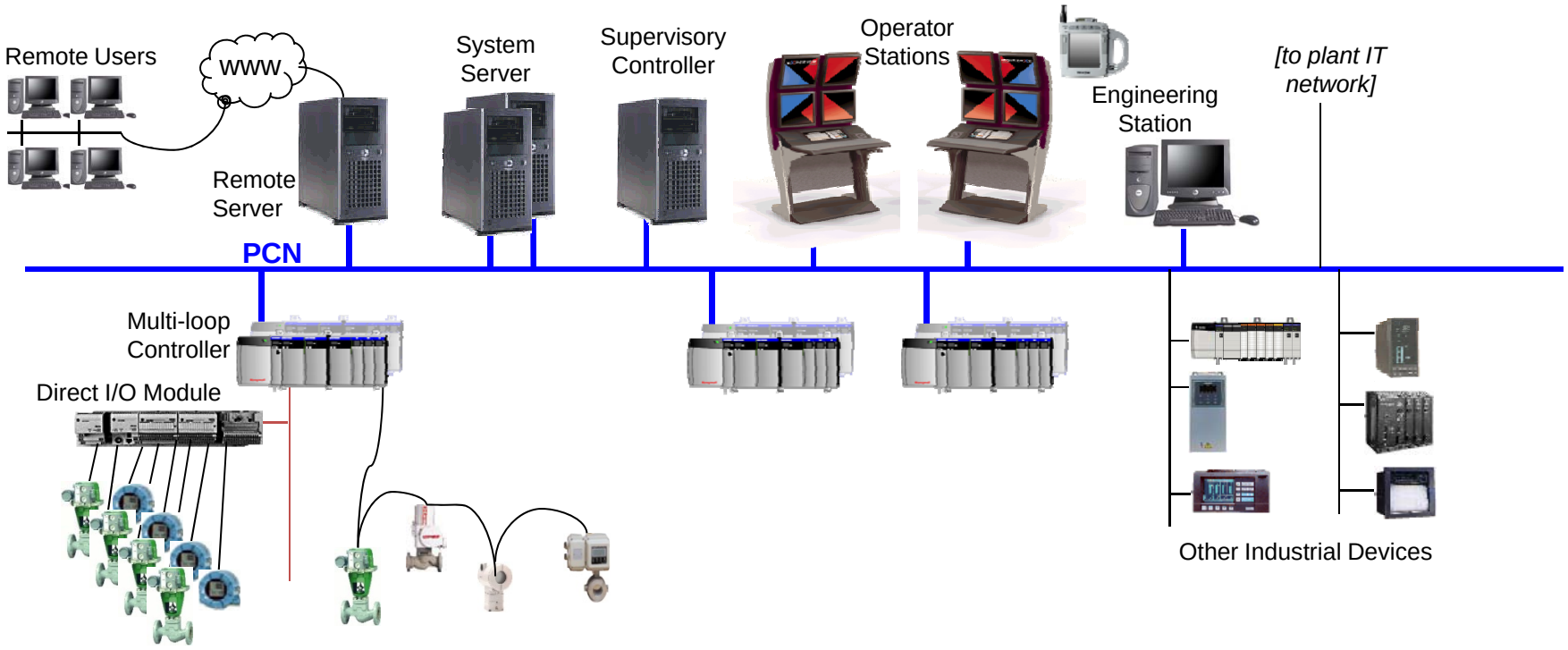


1990's COTS arrive on the scene

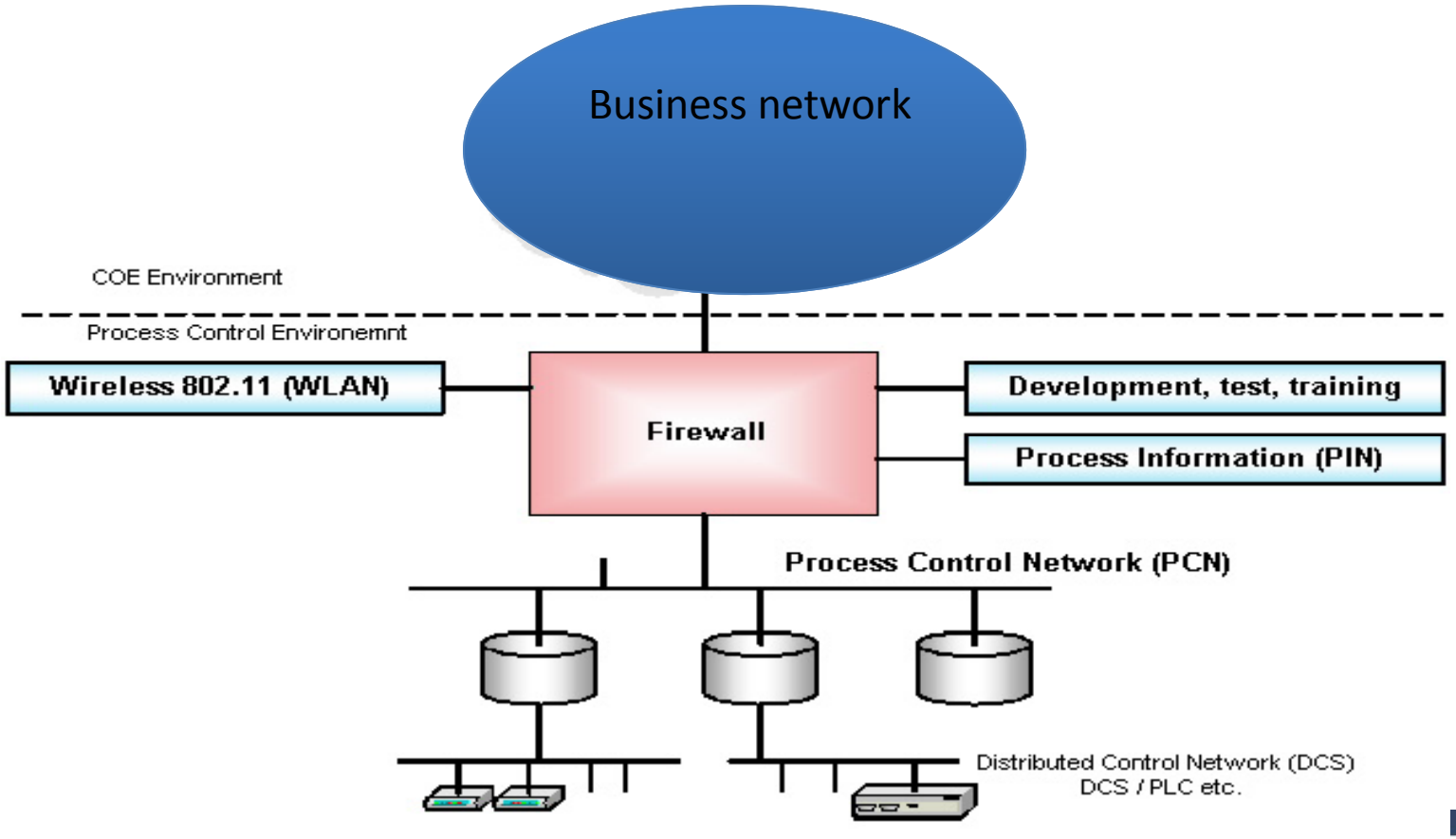


MESA INTERNATIONAL
MANUFACTURING ENTERPRISE SOLUTIONS ASSOCIATION
MESA.ORG

2000's Everything connected!



2001, Security Arrives



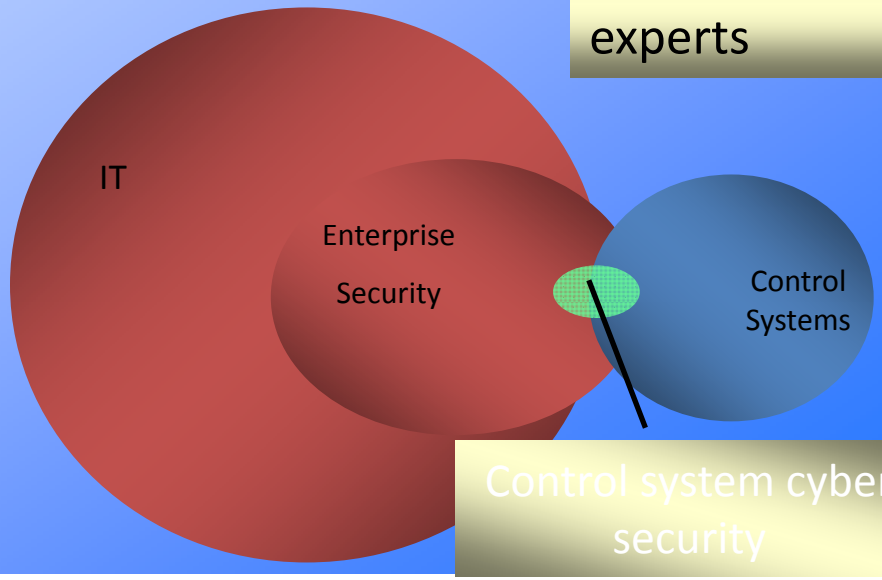
Cyber Security Overview

- Changing Compliance environment
  NERC CIP, ISO/IEC 17799, API 1164, NIST, ISA
- More aggressive organized Cyber threats
- "…a weapon of mass disruption.."

President Obama May 29, 2009

- Confluence of technologies

There are few industry experts



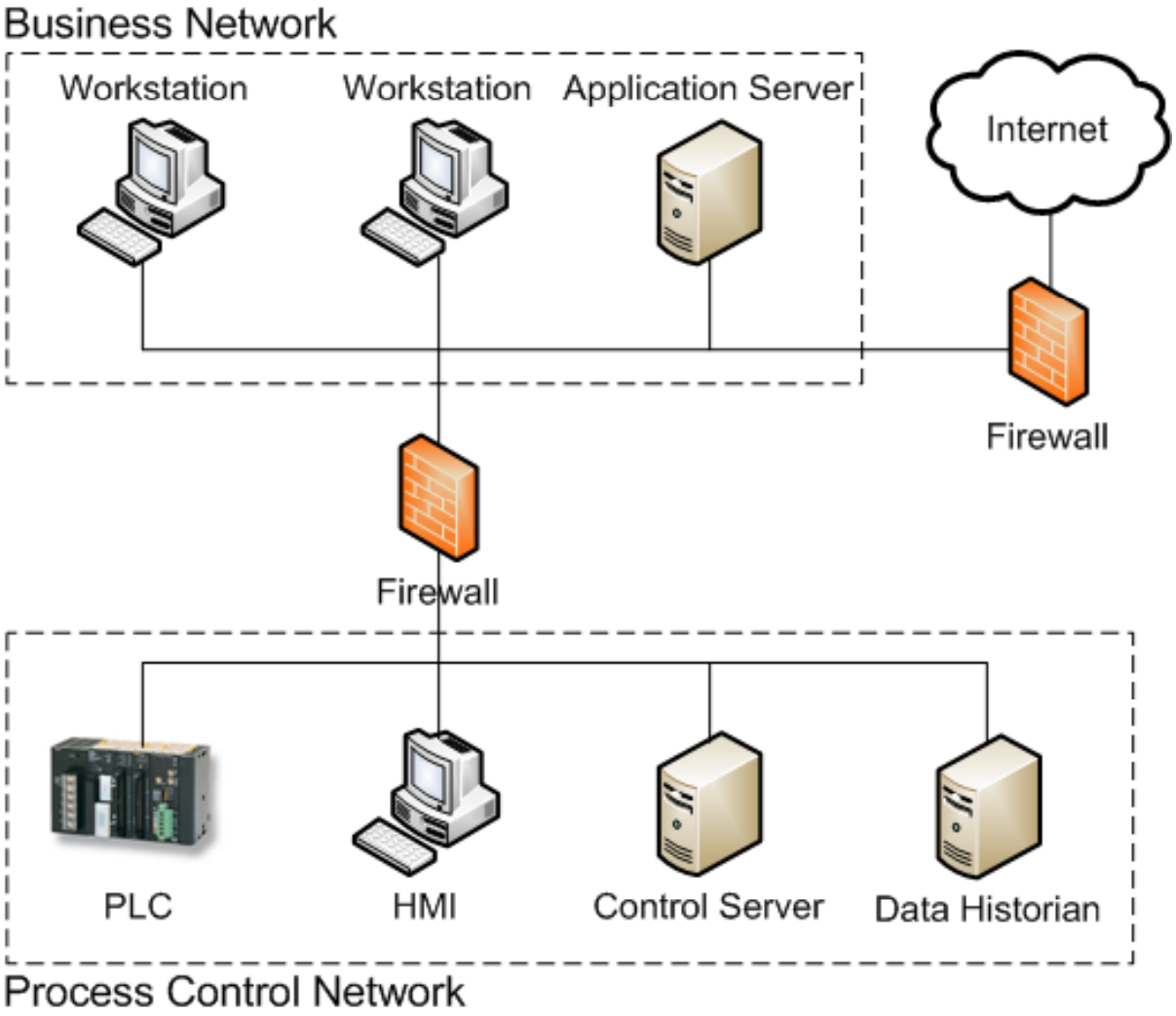
Control system cyber security

MESA INTERNATIONAL
MANUFACTURING ENTERPRISE SOLUTIONS ASSOCIATION
MESA.ORG

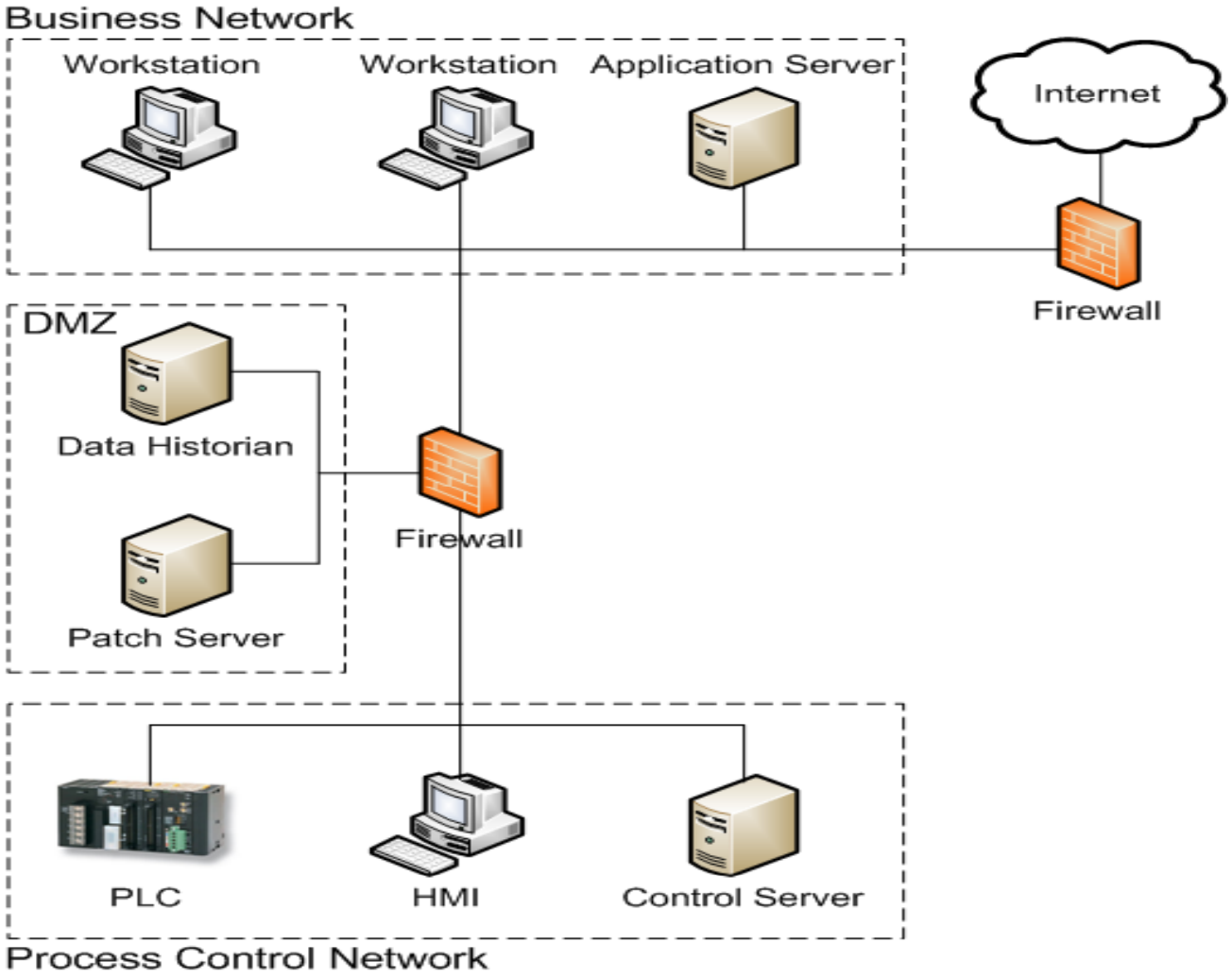
OVERVIEW OF ARCHITECTURE

MESA INTERNATIONAL
MANUFACTURING ENTERPRISE SOLUTIONS ASSOCIATION
MESA.ORG

Two-Tiered Network Architecture



Three-Tiered Network Architecture



WHY SECURITY?

Incident: Sewage Spill in Australia

- Between January 2000 and April 2000, the Maroochy Shire sewage treatment plant in Queensland, Australia experienced 47 unexplained faults.
- Millions of liters of raw sewage spilled out into local parks, rivers and even the grounds of a Hyatt Regency hotel.
- Marine life died, the creek water turned black and the stench was unbearable for residents, said Janelle Bryant of the Australian Environmental Protection Agency.

Incident: Sewage Spill in Australia

- On October 31, 2001, Vitek Boden was convicted of 26 counts of willfully using a restricted computer to cause damage and 1 count of causing serious environmental harm.
- Boden worked for the contractor involved in the installation of the sewage treatment plant in the state of Queensland in Australia. He left the contractor in December 1999 and approached the shire for employment. He was refused.
- Boden made at least 46 attempts to take control of the sewage system during March and April 2000. On April 23, the date of Boden's last hacking attempt, police who pulled over his car found radio and computer equipment.
- Later investigations found Boden's laptop had been used at the time of the attacks and his hard drive contained software for accessing and controlling the sewage management system.

Incident: Virus Attacks Train Signaling System

- In August 2003, a computer virus was blamed for bringing down train signaling systems throughout the eastern U.S. The signaling outage briefly affected the entire CSX system, which covers 23 states east of the Mississippi River.
- The virus infected the computer system at CSX Corp's Jacksonville, Fla., headquarters, shutting down signaling, dispatching, and other systems at about 1:15am EDT, CSX spokesman Adam Hollingsworth said, The cause was believed to be a worm virus similar to those that have infected the systems of major companies and agencies in recent days.

Incident: Gasoline Pipeline Rupture

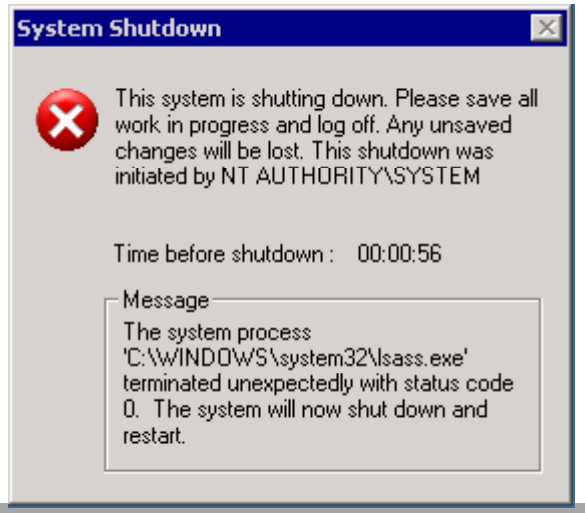
- In June 1999, a 16-inch-diameter steel pipeline owned by The Olympic Pipe Line Company ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington.
- About 1 1/2 hours after the rupture, the gasoline ignited and burned about 1 1/2 miles along the creek. Two 10-year-old boys and an 18-year-old young man died as a result of the accident. Eight additional injuries were documented.
- A single-family residence and the city of Bellingham's water treatment plant were severely damaged. Olympic estimated that total property damages were at least $45 million.

Incident: Gasoline Pipeline Rupture

- One of the causes of the accident was Olympic Pipe Line Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline.
- Shortly before the rupture, new records for pump vibration data were entered into the SCADA historical database. The records were created by a pipeline controller who had been temporarily assigned as a computer system administrator.
- According to the accident report, the database updates led to the system's becoming non-responsive at a critical time during pipeline operations.

Incident: Sasser Worm Disrupts Coastgaurd Computers in UK

- In May 2004, coastguard stations around the UK were severely disrupted after a computer worm brought down IT systems. The Sasser worm hit all 19 coastguard stations and the service's main headquarters, leaving staff reliant on paper maps and pens.
- The Maritime and Coastguard Agency said staff had reverted to manual map reading as soon as its computerized mapping systems started to fail. Coastguard staff were still able to use telephones and radios but fax and telex machines had been put out of action.



Accidental Incidents

- Accidental incidents remain a serious concern:
  - PLCs crashed by IT security audit.
  - DCS data feed causes gateway failure.
  - Duplicate IP address prevents machine startup.
  - IP address change shuts down chemical plant.

Today's threats?

- Targeted attacks
- Spearphising
- Employees

OVERVIEW OF ISA/IEC STANDARDS

MESA INTERNATIONAL
MANUFACTURING ENTERPRISE SOLUTIONS ASSOCIATION
MESA.ORG

Overview

- The Situation
- Chlorine Truck Loading Use Case
- Design & Risk Management Process
- Systems vs. Zones & Conduits
- Design Considerations
- Security Level Vector Discussion

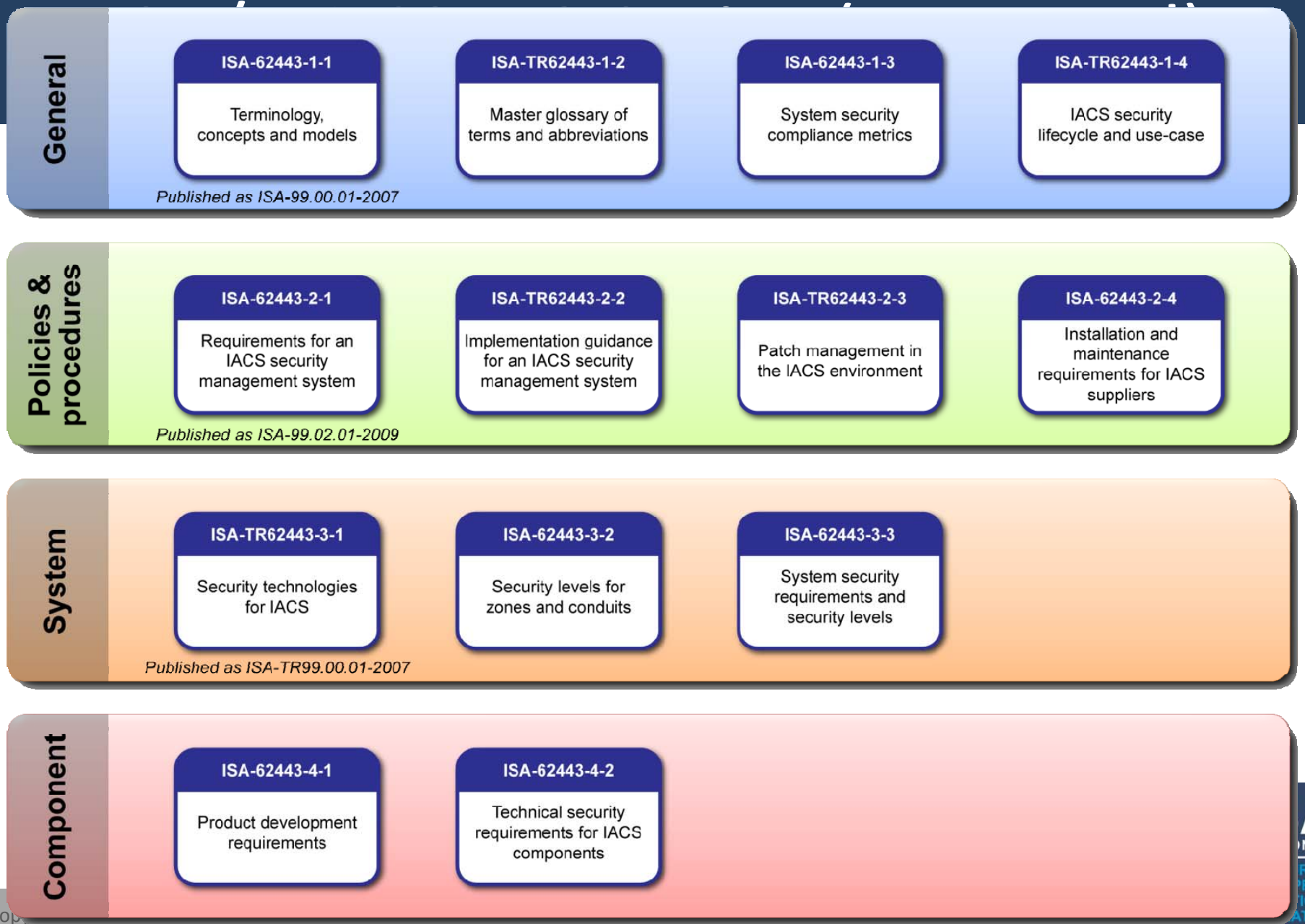
The Situation

- The Problem
  - With so many standards out there, how do you pick the best one?
  - Once you've picked a set of standards, how do you apply them?
- Security Standards
  - ISA/IEC 62443 (13)
  - ISO/IEC 2700x (10+)
  - NIST FIPS and SP800 (7+)
  - NERC CIP (8)
  - Smart Grid (?)

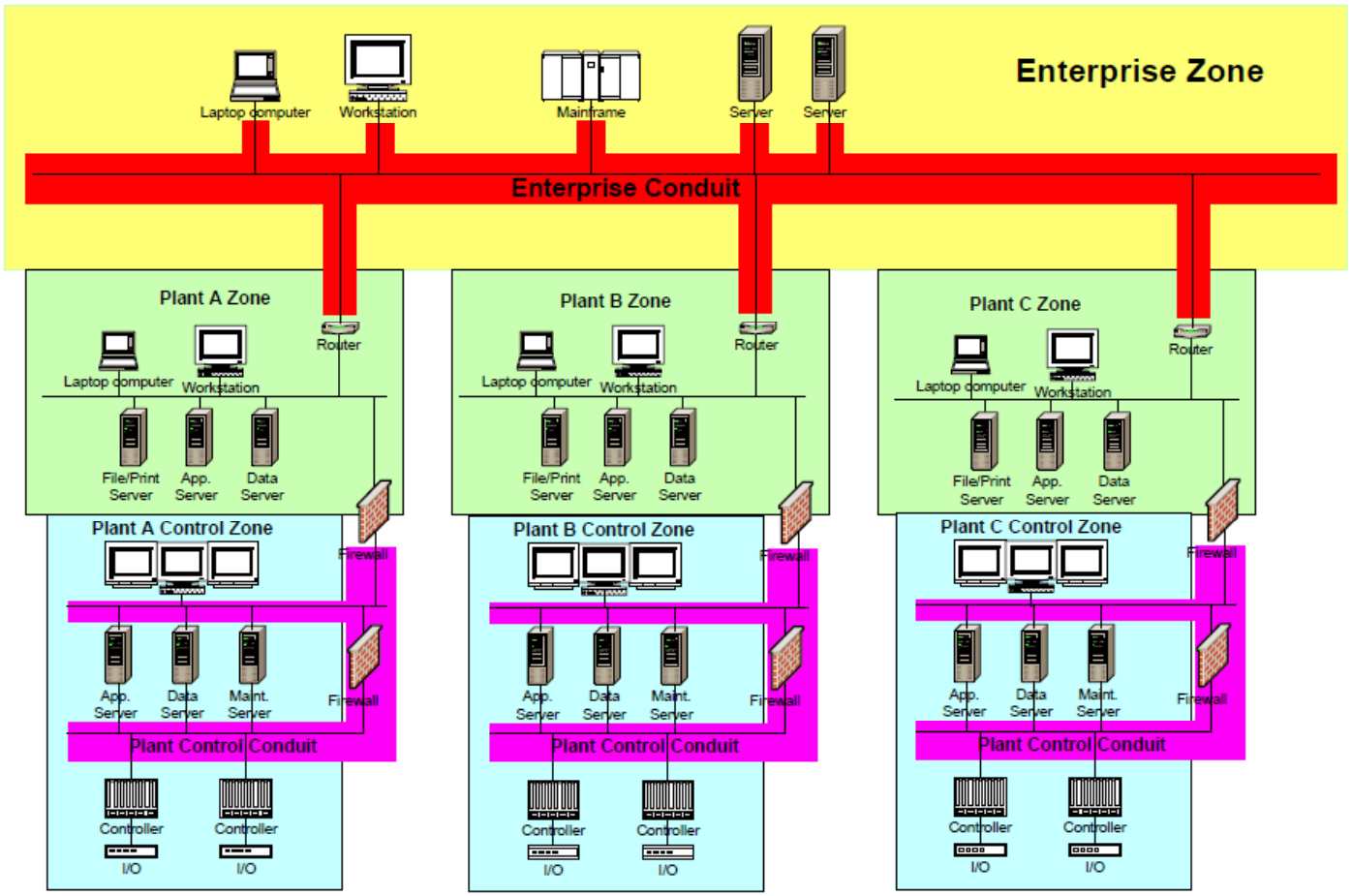
IT Standards

Sector-Specific Standards

- And that's just the security standards, then take into account the functional standards
  - Wireless = ISA 100.11a, WirelessHART, Zigbee, WiFi, Bluetooth…
  - Safety = ISA 84, IEC 61508/61511, DO-254, OSHA…
  - Management = ISO 9000, 14000, 31000, 50001, Six-Sigma…
  - And plenty of others…


General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Published as ISA-99.00.01-2007
Policies & procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Installation and maintenance requirements for IACS suppliers
Published as ISA-99.02.01-2009
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Published as ISA-TR99.00.01-2007
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components

Zones and Conduits



Security Standards

- Security standards generally tell you what has to be done or specified, but don't tell you how to go about doing it
  - Functional specifications
  - Security controls/countermeasures
- Some standards show a generic process, but leave it up to the reader to apply it in their case
- A few use-cases exist, but many times these are:
  - Sector-specific
  - Only apply in certain cases
  - Limited in scope
- Very few end-users discuss the details of their processes
  - Restrict information from potential attackers
- Almost no vendors or system integrators discuss the details of their processes
  - Restrict information from potential competitors

Chlorine Truck Loading Use Case

- Setting the Stage
  - ISA99 is trying to use a single use-case throughout the entire series to show how each part of the standard fits into the process
  - While the chlorine truck loading example is related to the chemical industry, the concepts presented could relate to any industry
  - The example allows for somewhat more realistic discussions of risk than in an IT-focused, DHS-focused, or purely hypothetical example
- Use case in early development and idea phase
  - Will take quite a long time to complete entire use-case
  - Different parts of use-case will probably emerge at different times

Chlorine Truck Loading Use Case: The Narrative

- Pharmaceutical Company XYZCorp
  - Wants to start producing new product (FixItAll)
  - No room for new production plant at existing facilities
  - Chemical process requires relatively small amounts of chlorine
  - Existing facility produces chlorine in large enough quantities
- XYZCorp considers their options
  - Conducts business assessment of building new facility
    - Existing facilities all near space capacity
    - New facility has good access to roads
    - Land is suitable and available
    - Existing chlorine production facility over 50 miles away
  - Considers options for transporting chlorine
    - Pipeline
    - Rail
    - Truck

Chlorine Truck Loading Use-Case: The Plan

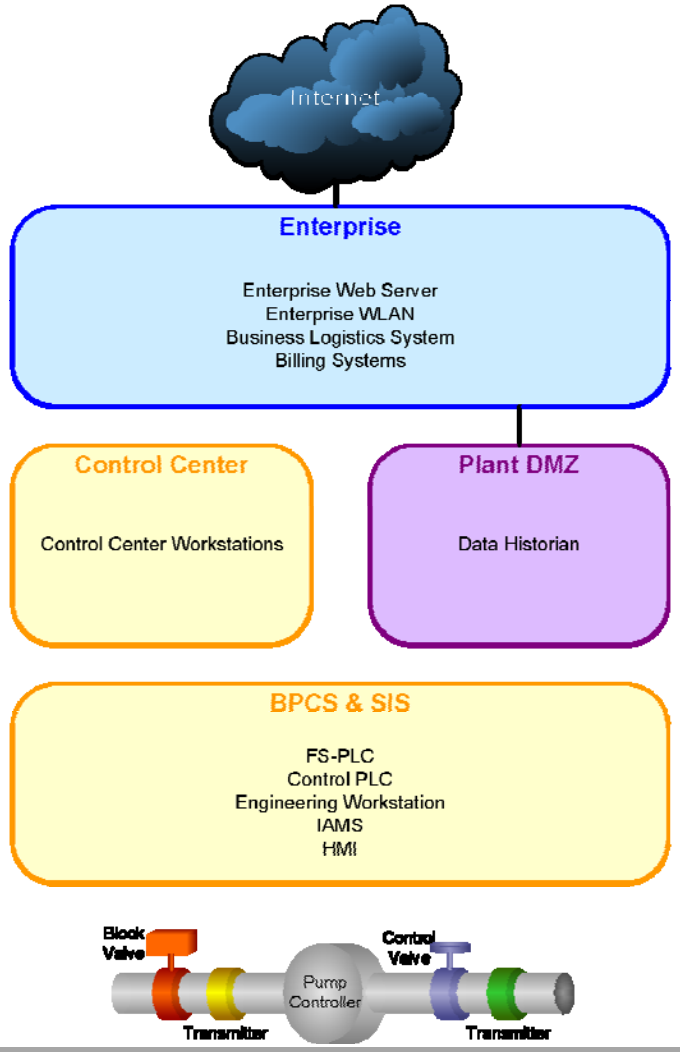
- Build truck loading/unloading facilities
  - Loading @ existing facility, unloading @ new facility
  - Unmanned except during loading/unloading operations
  - Hazardous chemical requires special handling & safety
- Generations of equipment
  - Existing facility uses legacy equipment (brown-field)
  - New facility designed with current technology (green-field)
- Facility monitoring & control
  - Unmanned – centralized monitoring @ control center
  - Manned & operational – local control with both local & centralized monitoring
- Attached to business systems
  - Billing & logistics
  - Inventory tracking

Chlorine Truck Loading Use Case: Design Considerations

- Systems needed
  - Safety Instrumented System (SIS)
  - Basic Process Control System (BPCS)
  - Control center
  - Plant DMZ
  - Enterprise systems
- Level of SIS integration with BPCS?
  - Air-gapped
  - Interfaced
  - Integrated

Initial Design Process: Identify the Control Assets

- Process Equipment
  - Pump Controller
  - Transmitters
  - Block and Control Valves
- BPCS & SIS
  - Functional Safety-PLC
  - Control PLC
  - Engineering Workstation(s)
  - Instrument Asset Management System
  - Human-Machine Interface(s)
- Control Center
  - Control Center Workstations
- Plant DMZ
  - Data Historian
- Enterprise
  - Enterprise Web Server
  - Enterprise WLAN
  - Business Logistics System
  - Billing System



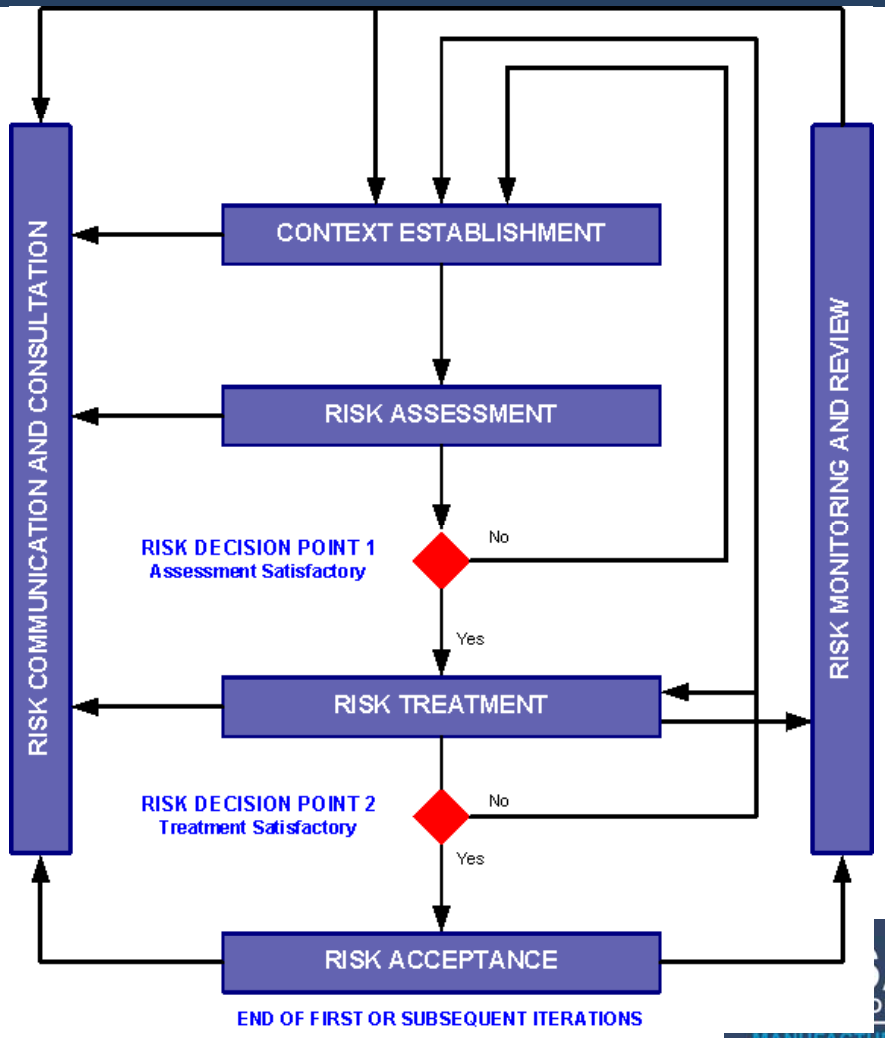
NOW WHAT???

Design Process

- Now that the business case and some initial design ideas have been put down, where do you go from here?
  A. Design the control system without worrying about the security?
  B. Design everything so secure that it becomes unusable?
  C. Throw in firewalls everywhere?
  D. Conduct a detailed risk assessment at the device level?
  E. Conduct a multi-stage risk assessment starting with the top level and working down to the low level as the design progresses?
- Generally, the ISA99 approach begins with E

Modified ISO/IEC 27005 Risk Management Process

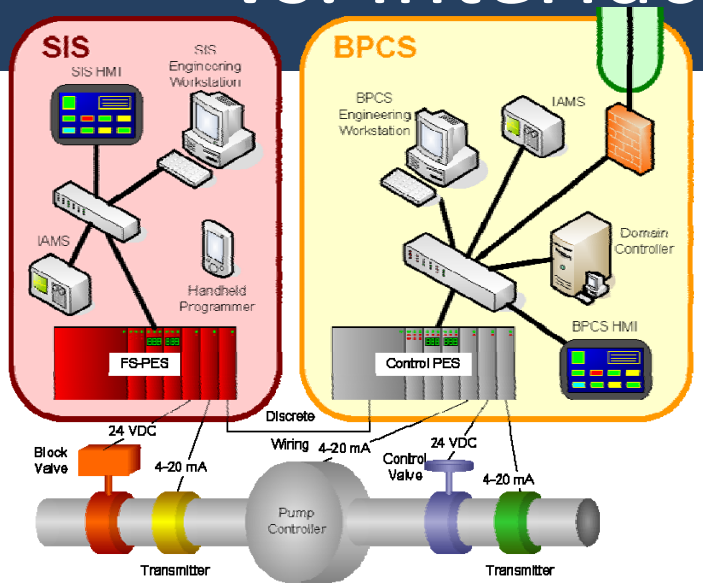
- ISA99, Working Group 2 working on modified ISO/IEC 27005 risk management process
  - Uses basic shell from 27005
  - Modifies it for multi-stage risk assessment process
  - Discusses “jump-in” point
  - Relates risk management process to overall cyber security management system design process
    - Business planning
    - Change management
    - Decommissioning

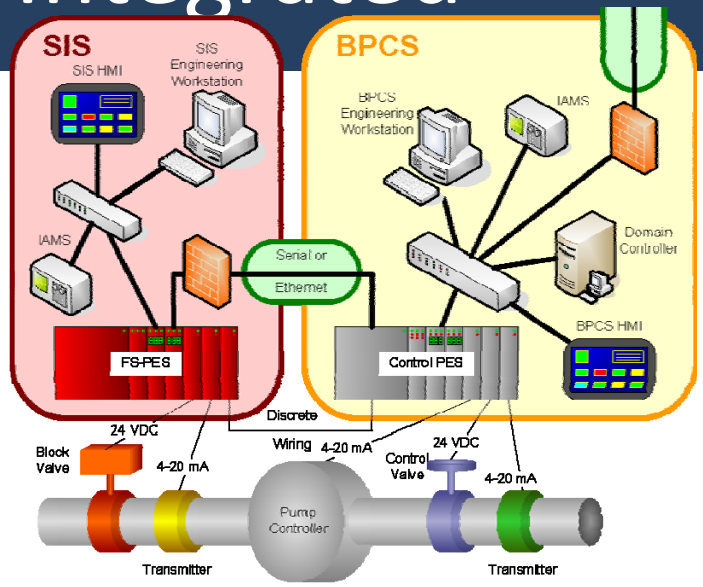


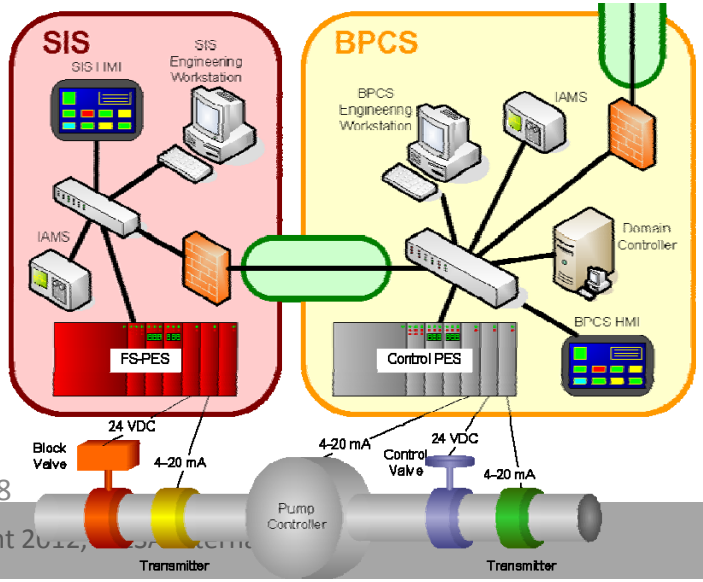
Systems vs. Zones & Conduits

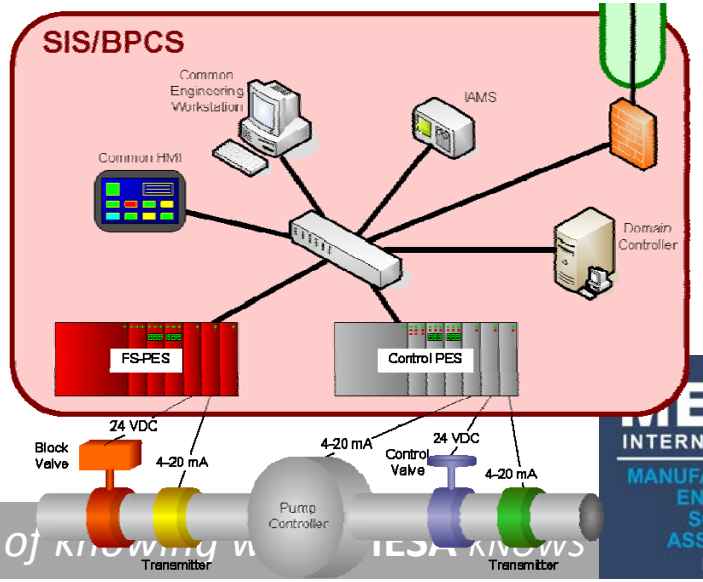
- Systems ≠ Zones
  - Conducting a system breakdown may give some indication of future zones, but there is no direct one-to-one correlation between the two
  - Systems = Collections of equipment/assets that logically function together to perform at least one task
  - Zones = Collections of equipment/assets that logically have similar security requirements
- System breakdown helps to identify different sets of equipment during the risk assessment phase
- Zones are created after the risk assessment phase based on the particular security requirements for that set of equipment/assets
- Conduits are a special kind of zone containing a communication channel

Design Considerations: SIS Air-Gapped vs. Interfaced vs. Integrated



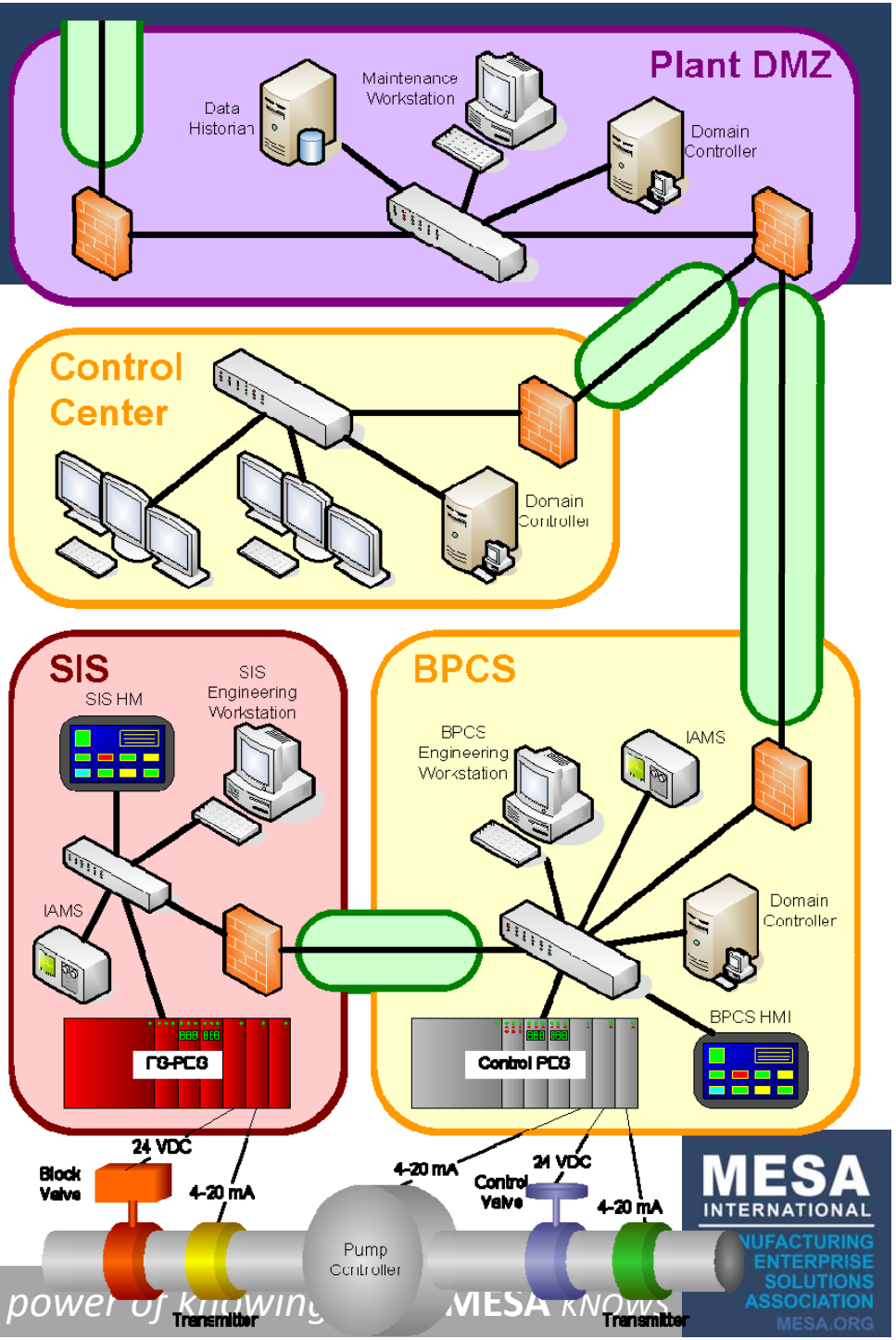






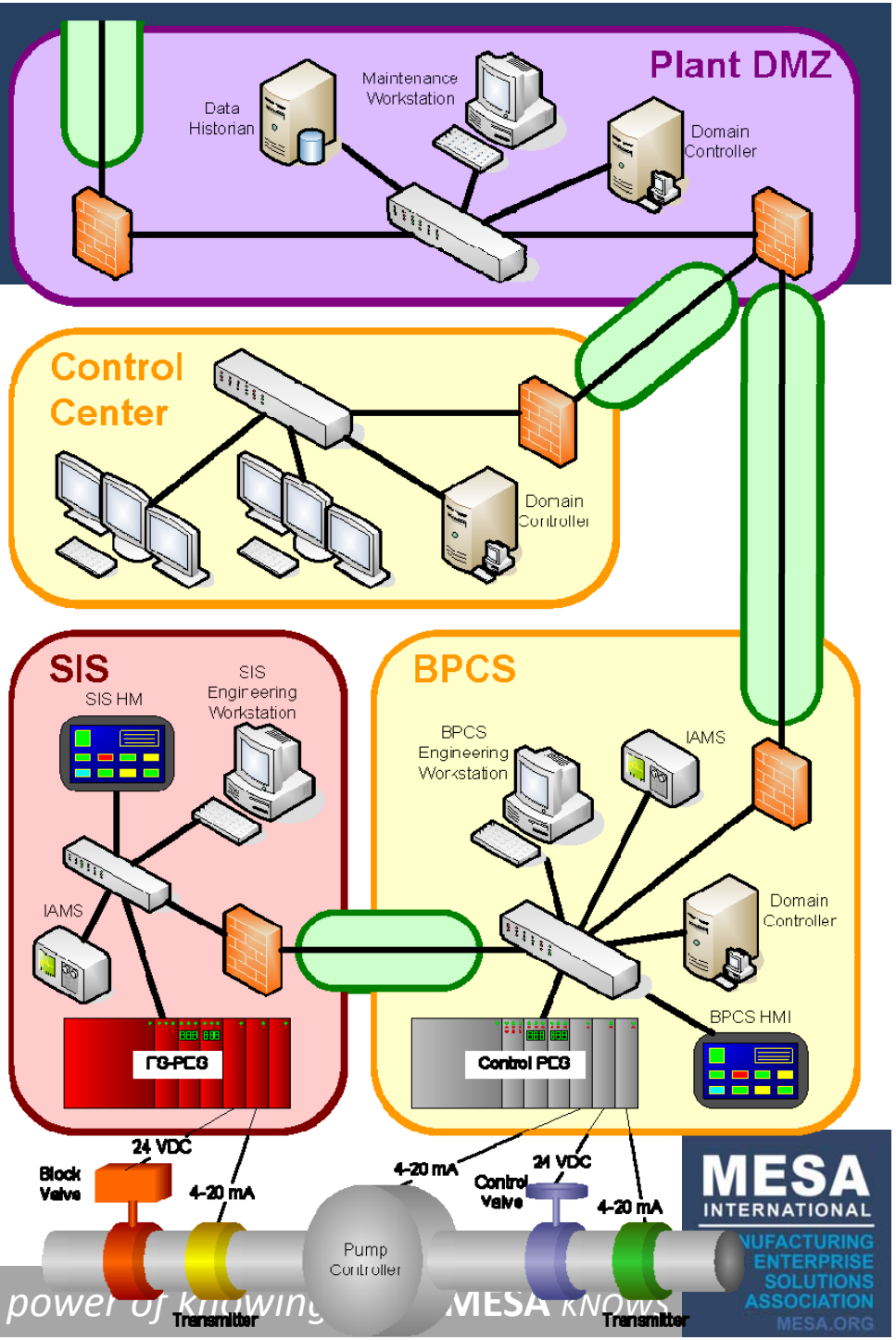
Security Level Vector Discussion

- Industrial Security Isn't Always About Death & Dismemberment
  - Some security concepts don't fit into that model
- Use the Foundational Requirements to Engineer the System Security
  - Identification & Authentication Control
  - Use Control
  - System Integrity
  - Data Confidentiality
  - Restricted Data Flow
  - Timely Response to Events
  - Resource Availability



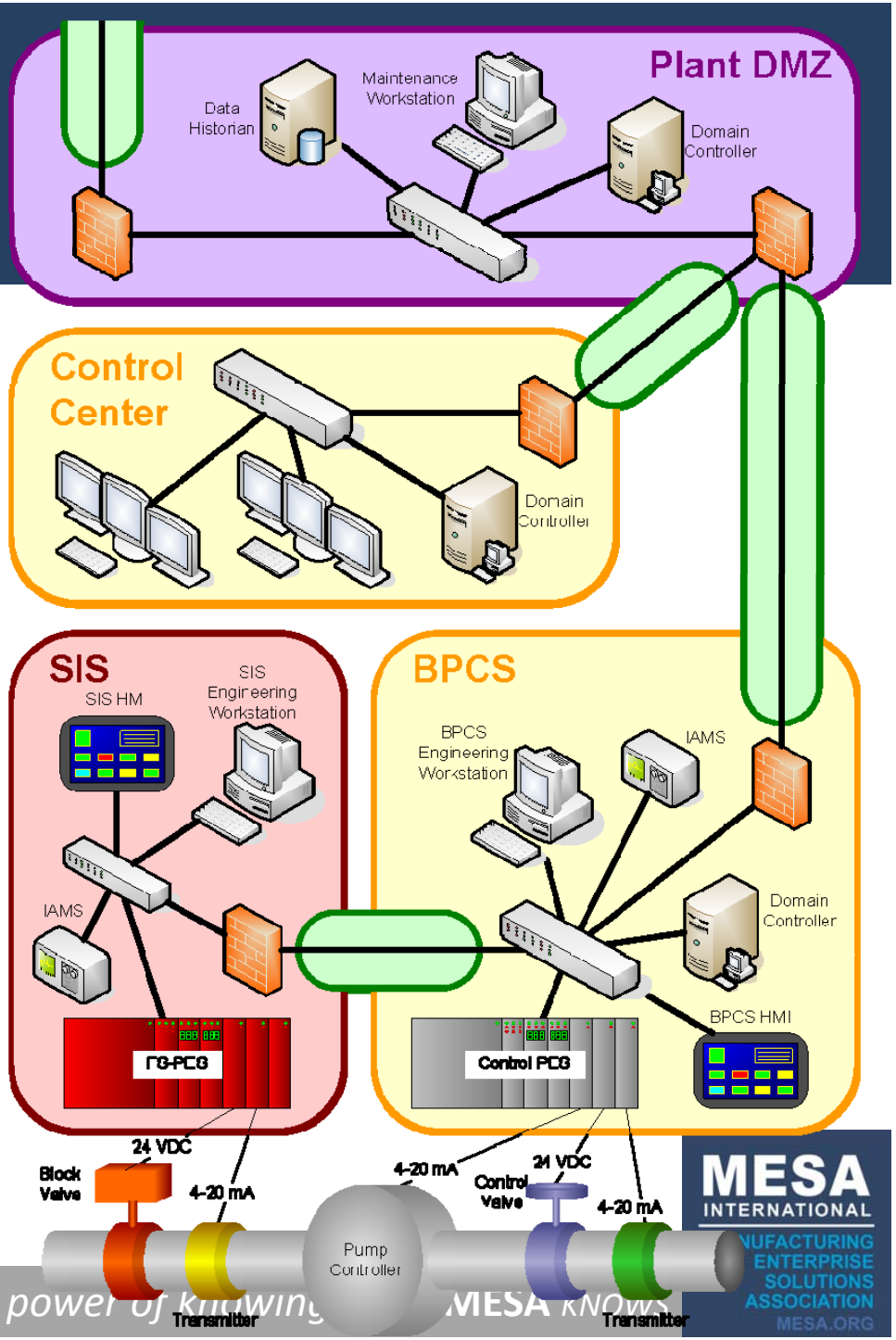
Security Level Vector Discussion

- How will the switches affect the security of the BPCS & SIS?
  - High availability is fairly common
  - Uncommon for switches to have good access control (natively)
  - Confidentiality depends, is SNMP enabled AND secured?
  - If switch fails completely, what happens to system integrity? What about intermittent failures, or bad ports? What are the safety implications?

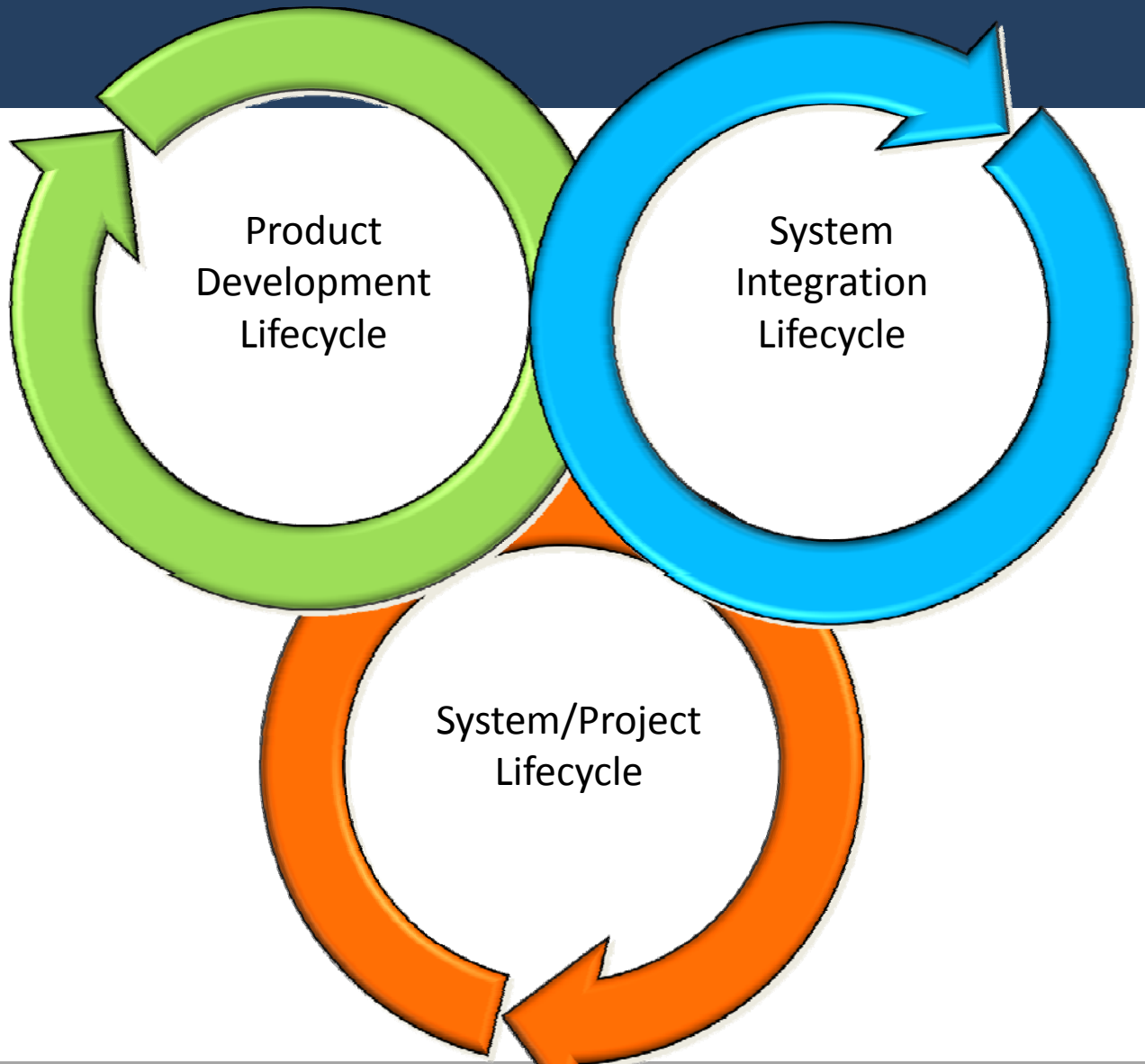


Security Level Vector Discussion

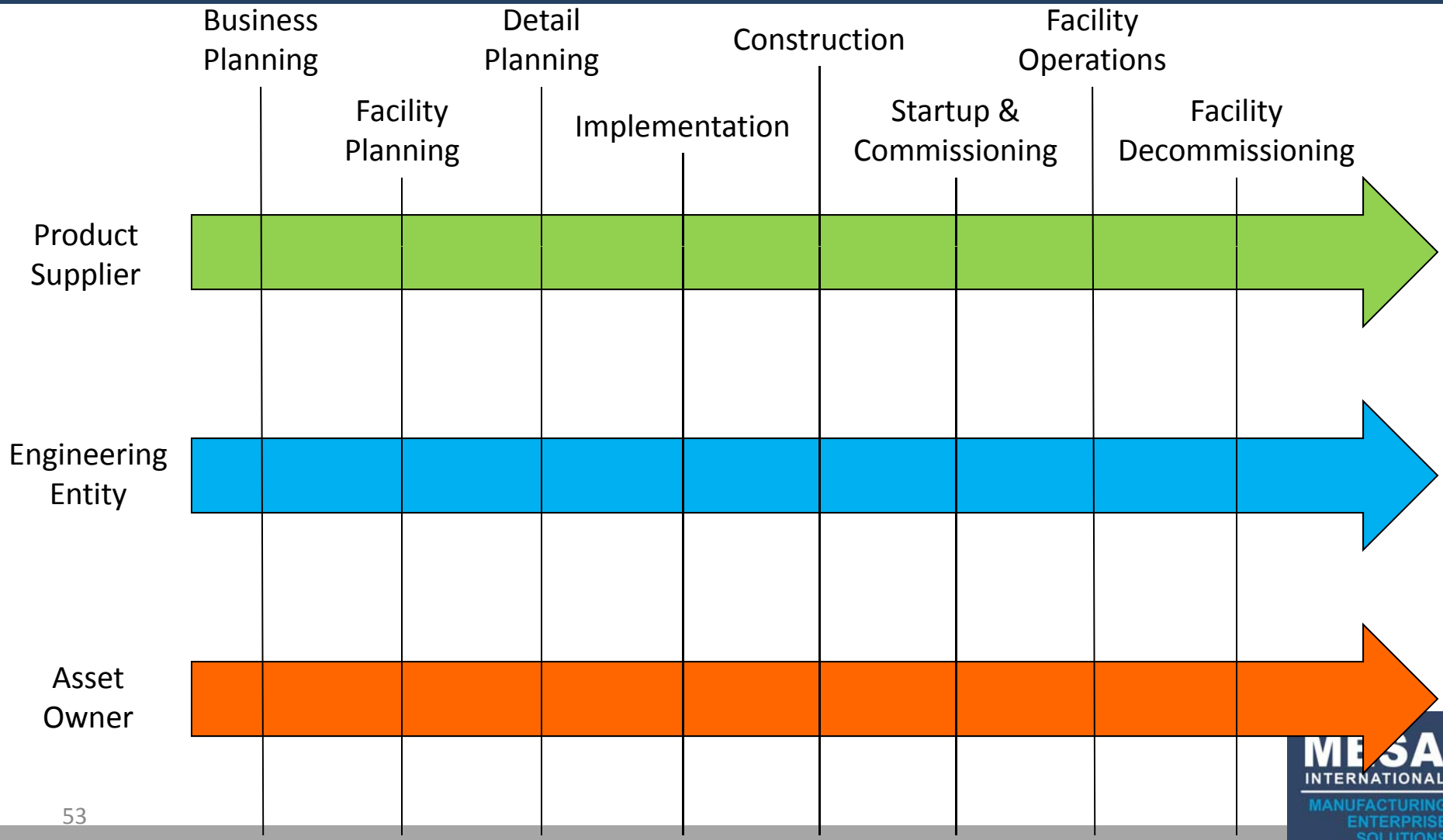
- Now, what about other components?
- How do each of the component capabilities roll into a system capability?
  - Mathematical/Additive?
  - Qualitative assessment of capabilities?
- How do capabilities relate to achieved security levels?



Security Lifecycles

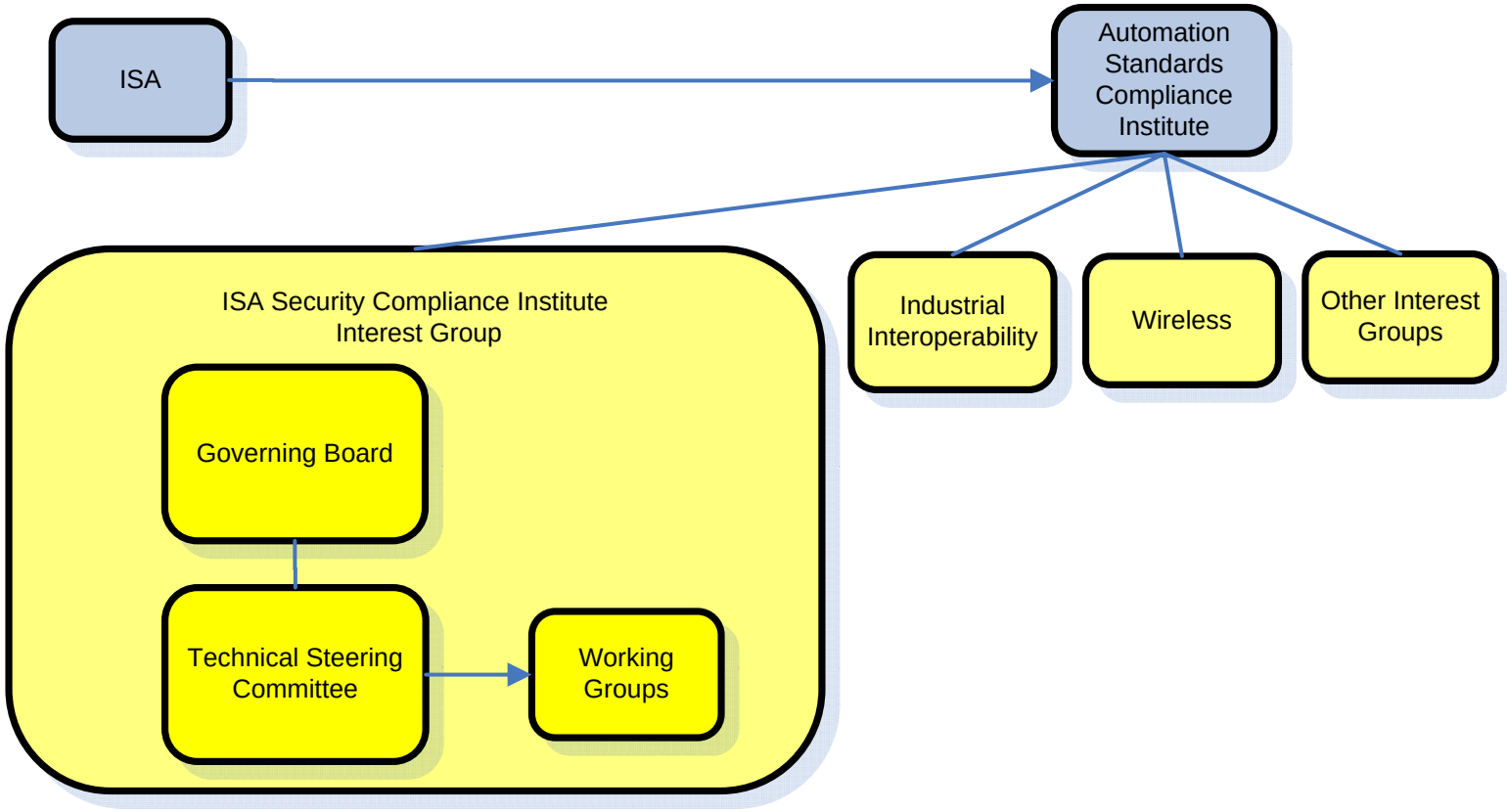


Security Lifecycle



ISA SECURITY COMPLIANCE INSTITUTE (ISCI) ORGANIZATION

An ISA Owned Organization



ISA Security Compliance Institute (ISCI)

Who We Are

Consortium of Asset Owners, Suppliers, and Industry Organizations formed in 2007 under the ISA Automation Standards Compliance Institute (ASCI):

Mission

Establish a set of well-engineered specifications and processes for the testing and certification of critical control systems products

Decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders

ISCI Member Companies

- ISCI membership is open to all organizations
  - Strategic membership level
  - Technical membership level
  - Informational membership level

- Current membership
  - Chevron
  - Egemin
  - exida
  - ExxonMobil
  - Honeywell
  - Invensys
  - Siemens
  - Yokogawa
  - IPA
  - ISA99/ISCI Joint Working Group Liaison

57

ISASecure Designation

- Trademarked designation that provides instant recognition of product security characteristics and capabilities.
- Independent Industry stamp of approval.
- Similar to 'Safety Integrity Level' Certification (ISO/IEC 61508).

ANSI/ACLASS Accredited Conformance Scheme

ISASecure Embedded Device Security Assurance (EDSA) certification accredited as an ISO/IEC Guide 65 conformance scheme by ANSI/ACLASS. This includes both ISO/IEC 17025 and ISO/IEC 17011.

Go to www.ansi.org/isasecure for details.

1. Provides global recognition for ISASecure certification
2. Independent CB accreditation by ANSI/ACLASS
3. ISASecure can scale on a global basis
4. Ensures certification process is open, fair, credible, and robust.

Why Do We Need Secure Devices

- Increased Industrial Control System exploits and attacks
  - Stuxnet
  - Nearly 40 exploits released recently
- Hacker conferences starting to have control system tracks
  - Black Hat
  - Hacker Halted
- Control systems using standard IT devices

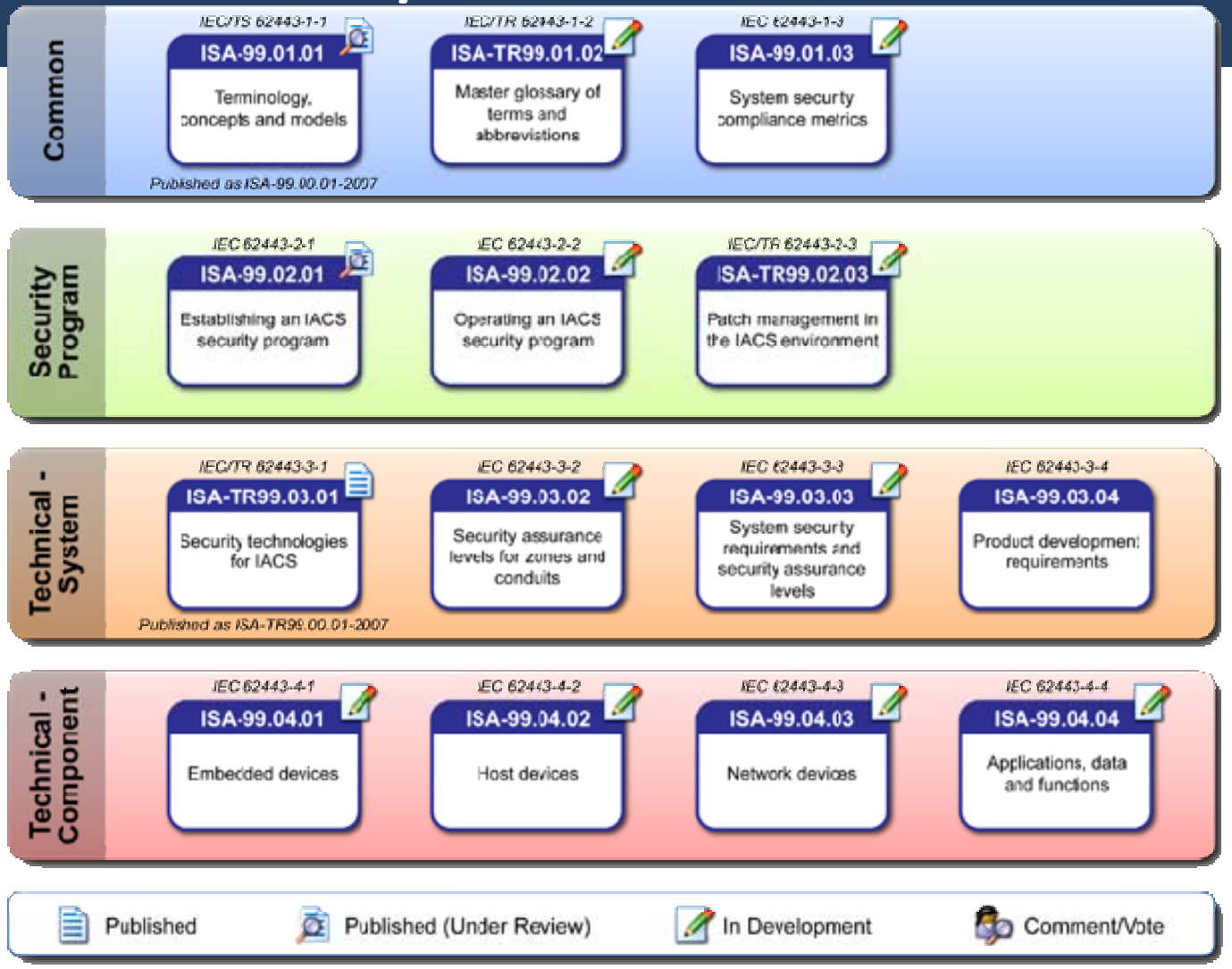
ISASecure Certification Specification Process

- ISCI board defines scope and work process
- Technical steering committee manages working groups who draft specifications
- Specifications reviewed by external 3rd party if required
- Voted and approved by full ISCI voting membership
- Approved specifications adopted by ISCI Governing Board and posted on website
- Specifications developed to-date have been donated to ISA for submission to the ISA99 Standards Committee

ISASecure Vendor Device Approval Process

- Vendor submits device to ANSI ACLASS charted lab
- Charted lab completes three part assessment
  - Physically evaluates device for functional security (FSA)
  - Conducts communication robustness test (CRT) using ISCI- appoved test tool
  - Charted lab completes vendor audit (SDSA) on software development practices
- Charted lab issues final assessment report and certification upon successful test and audit

ISA 62443/99 Work Products



ISCI Program Outreach

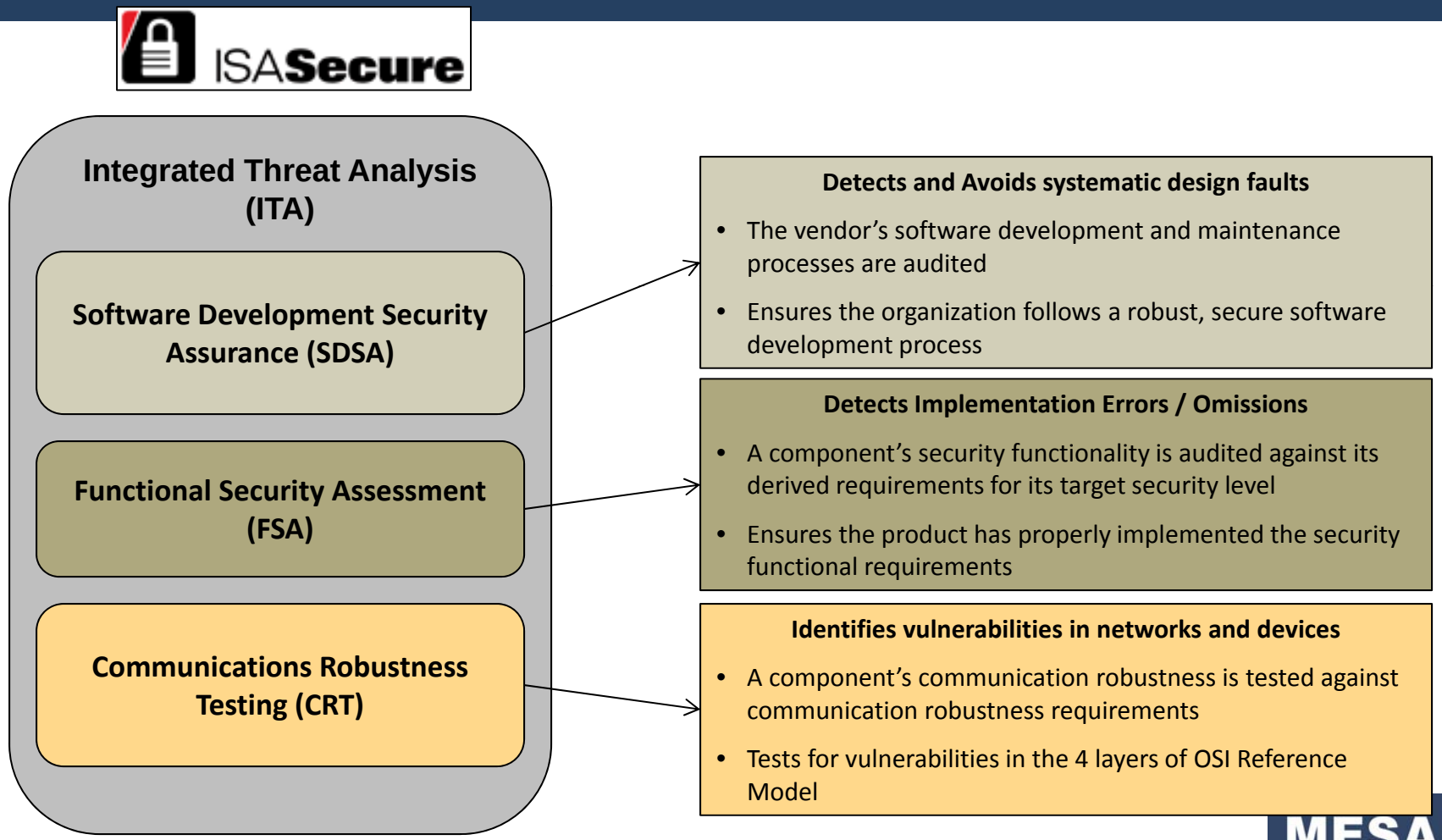
- Website www.isasecure.org
- *ISASecure* EDSA Certification Specifications and Program Definition Documents Approved and posted for public access at www.isasecure.org
- ISCI Board donated EDSA FSA and SDSA technical specification to ISA-99 Committee via ISA99-ISCI Joint Working Group
- Webinar Series throughout 2011

ISASECURE EMBEDDED DEVICE SECURITY ASSURANCE PROGRAM

Embedded Device

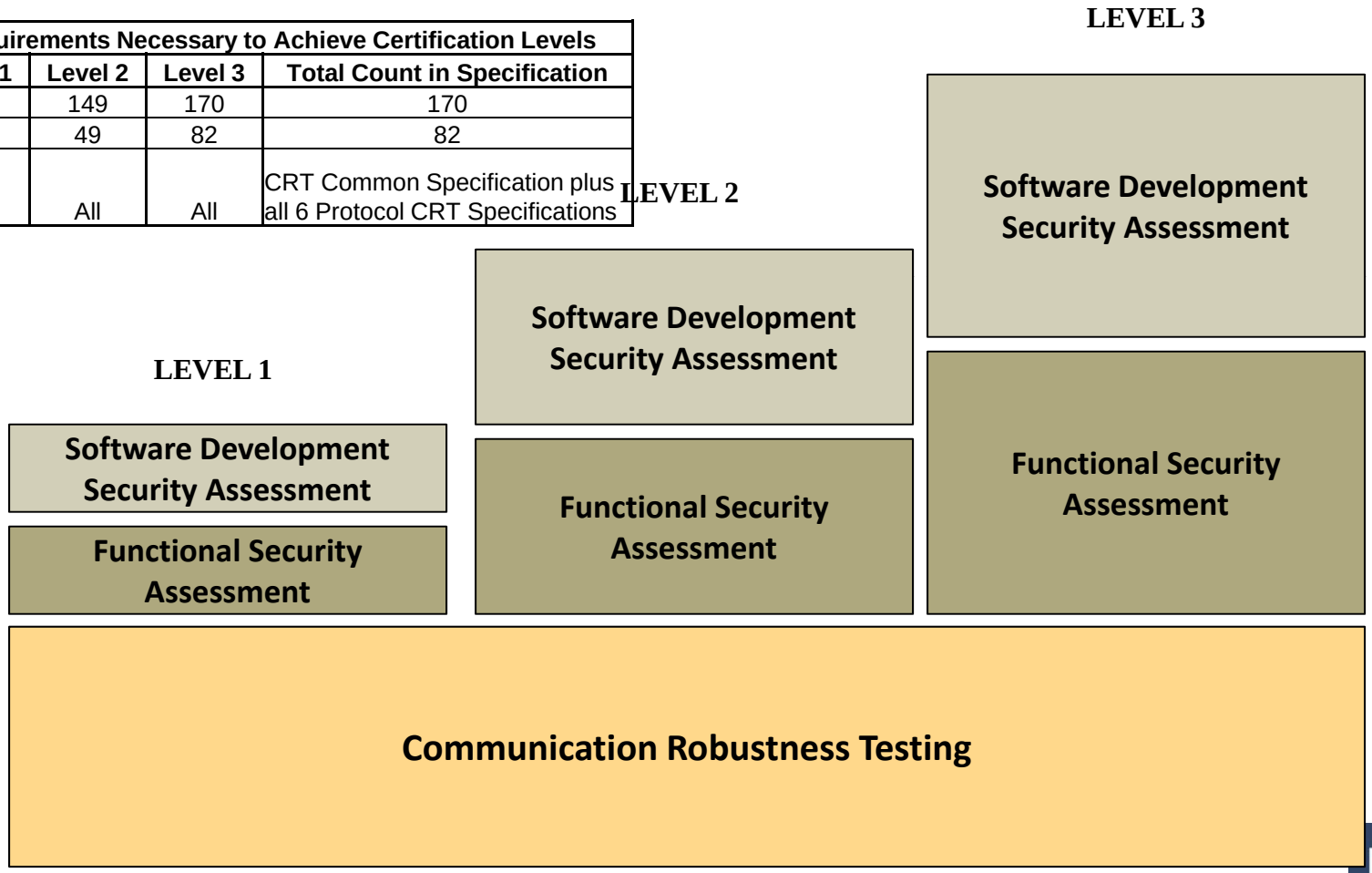
- Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process
- Examples:
  - Programmable Logic Controller (PLC)
  - Distributed Control System (DCS) controller
  - Safety Logic Solver
  - Programmable Automation Controller (PAC)
  - Intelligent Electronic Device (IED)
  - Digital Protective Relay
  - Smart Motor Starter/Controller
  - SCADA Controller
  - Remote Terminal Unit (RTU)
  - Turbine controller
  - Vibration monitoring controller
  - Compressor controller

Embedded Device Security Assurance Certification



ISASecure Levels

	Requirements Necessary to Achieve Certification Levels			
	Level 1	Level 2	Level 3	Total Count in Specification
SDSA	130	149	170	170
FSA	20	49	82	82
CRT	All	All	All	CRT Common Specification plus all 6 Protocol CRT Specifications



MESA INTERNATIONAL
MANUFACTURING ENTERPRISE SOLUTIONS ASSOCIATION
MESA.ORG

Communications Robustness Test (CRT)

- Measures the extent to which network protocol implementations on an embedded device defends themselves and other device functions against unusual or intentionally malicious traffic received from the network.
- Inappropriate message response (s), or failure of the device to continue to adequately maintain essential services, demonstrates potential security vulnerabilities within the device.

Communication Robustness Testing

Functional Security Assessment (FSA)

Security Feature Tests

Purpose:

- Verification and validation that the device or system under test incorporates a minimum set of security features needed to counteract common security threats

Composition

- Set of requirements, derived from existing reference standards and traceable to source standard
- One or more acceptable solutions (countermeasures) identified for each requirement
- If applicable, procedures to verify the requirement has been satisfied

Software Security Development Assessment

Secure Software Engineering

Purpose:

- Verification and validation that software for the device or system under test was developed following appropriate engineering practices to minimize software errors that could lead to security vulnerabilities

Composition

- Set of requirements, derived from existing reference standards and traceable to source standard (IEC 61508, ISO/IEC 15408)
- One or more acceptable arguments identified for each requirement

Software Development Security Assessment

Security Development Lifecycle

Security Management Process	This phase specifies a process for planning and managing security development activities to ensure that security is designed into a product. For example, this phase incorporates requirements that the development team have a security management plan and that the developers assigned to the project are competent and have been provided basic training in good security engineering practices and processes. Also includes requirements that the project team creates and follows a configuration management plan.
Security Requirements Specification	Most vulnerabilities and weaknesses in software intensive information systems can be traced to inadequate or incomplete requirements. This phase requires that the project team document customer driven security requirements, security features and the potential threats that drive the need for these features.
Software Architecture Design	Software architecture facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects. This phase requires the project team develop a top-level software design and ensures that security is included in the design.
Security Risk Assessment and Threat Modeling	This phase requires the project team determine which components can affect security and plan which components will require security code reviews and security testing. Also requires that a threat model be created and documented for the product.
Detailed Software Design	This phase requires the project team design the software down to the module level following security design best practices.
Document Security Guidelines	This phase requires the project team create guidelines that users of the product must follow to ensure security requirements are met.
Software Module Implementation & Verification	This phase requires the project team implement design by writing code following security coding guidelines. It ensures that software modules are implemented correctly by conducting security code reviews, static analysis and module testing.
Security Integration Testing	This phase requires that the project team perform security specific tests such as fuzz testing and penetration testing.
Security Process Verification	This phase requires an independent assessment that all required software development processes have been followed
Security Response Planning	This phase requires the project team establish a process to be able to quickly respond to security issues found in the field if and when they happen.
Security Validation Testing	This phase requires that the project team confirm that all security requirements have been met preferably by test or by analysis.
Security Response Execution	This phase requires the project team respond to security problems in the field by taking action to both preventative and corrective action.

EDSA Certification Process

Typical Chartered Lab Level of Effort in Man Weeks

		Level 1	Level 2	Level 3
1.	CRT test all accessible TCP/IP interfaces	1 - 2 weeks	1 - 2 weeks	1 - 2 weeks
2.	Perform FSA on device and all interfaces	< 1 week	1 week	1 – 2 weeks
3.	Audit supplier's software development process	1 week	1 – 2 weeks	1 – 2 weeks
4.	Perform ITA and issue report	1 week	1 week	1 week
		3 – 5 weeks	4 – 6 weeks	4 – 10 weeks

WHY *ISASECURE*?

Benefits

End-user

- Easy to specify
- Build security requirement into RFP
- Reduced time in FAT/SAT
- Know security level out of the box

Supplier

- Evaluated once
- Recognition for effort
- Build in security
- Product differentiator

WHO TO CONTACT FOR MORE INFORMATION

Who to Contact to Certify Products

ISASecure EDSA Chartered Lab

exida
John Cusimano
Director of Security Services
Phone: (215) 453-1720
Fax: (215) 257-1657
Email: jcusimano@exida.com
Website: http://www.exida.com

Who to contact for CRT Test Tool

http://www.wurldtech.com

Wurldtech Security Technologies, Inc.

Greg Maciel

Achilles Sales Manager

Phone: (949) 300-4040

Email: gmaciel@wurldtech.com

Who to contact for ISCI Membership

Andre Ristaino

Managing Director, ASCI

Direct Phone: 919-990-9222

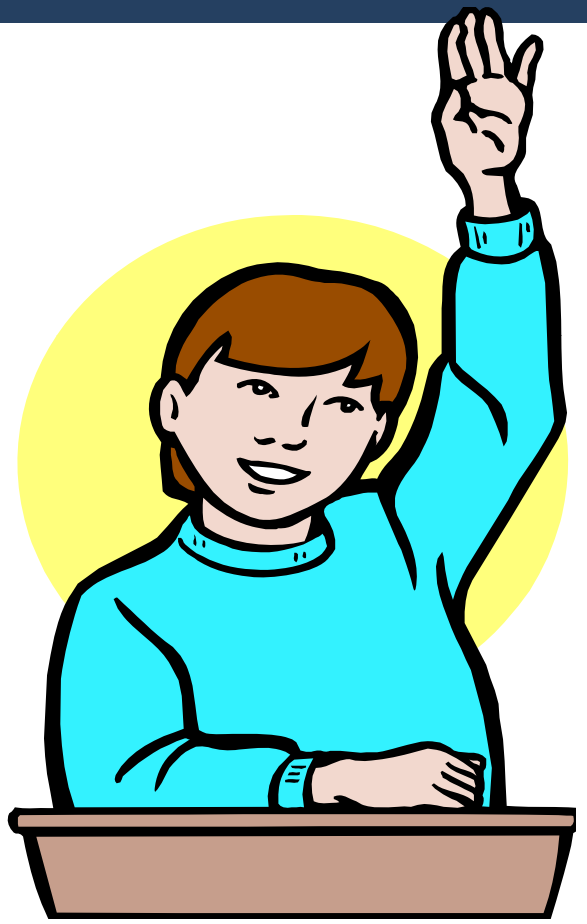
Fax: 919-549-8288

Email: aristaino@isa.org

Website: http://www.isasecure.org

Q&A

Questions?



Thank you

20 YEARS & KNOWING

OUR MEMBERS ARE THE MOST AGILE COMPANIES IN THE WORLD.
THEY KNOW THEY HAVE A RESPONSIBILITY TO INDUSTRY AND TO ONE ANOTHER.
THEY KNOW THE CONSEQUENCES OF AVOIDING A SINGLE IMPROVEMENT CAN MEAN MILLIONS OF DOLLARS AND A POSSIBLE GLOBAL IMPACT.
THEY KNOW THE POWER OF KNOWING WHAT MESA KNOWS.

"We saved $2.4 million because our operations team was able to make a case for improvement with resources from **MESA**."

Global Education Program

MESA has trained over 500 professionals and provides 800+ pieces of content valued at over $13 million dollars.

"At the Global Education Programs, I learn from mistakes and successes of other manufacturers, I network with the best, AND the cost is credited to my membership fees. Becoming a member was a no-brainer."

MESA *KNOWS*

SUSTAINABILITY & ECO-EFFICIENCY - LEAN - METRICS & PERFORMANCE MANAGEMENT
INFORMATION INTEGRATION - SAFETY - ASSET PERFORMANCE MANAGEMENT - B2MML
QUALITY & COMPLIANCE - PRODUCT LIFECYCLE MANAGEMENT - AUTOMATION

Manufacturers • Producers • Systems Integrators • Consultants

DO YOU KNOW MESA?

MESA International Headquarters 107 S. Southgate Drive, Chandler, AZ 85226 USA
+1 480 893 6883 | hq@mesa.org | www.MESA.org